

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 1 0 日
Date of Application:

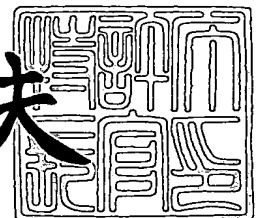
出 願 番 号 特 願 2 0 0 3 - 3 1 8 4 7 5
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 3 1 8 4 7 5]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0304622
【提出日】 平成15年 9月10日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 12/00 537
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 斉藤 敦久
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 金井 洋一
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-299714
 【出願日】 平成14年10月11日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-299721
 【出願日】 平成14年10月11日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

電子ファイルを格納する電子ファイル格納領域と、

上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、

上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有することを特徴とする電子ファイル管理装置。

【請求項 2】

上記電子ファイル管理手段は、

上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納することを特徴とする請求項 1 記載の電子ファイル管理装置。

【請求項 3】

上記電子ファイル管理手段は、

上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルを格納する代わりに、その保護電子ファイルを上記電子ファイル格納領域に格納することを特徴とする請求項 1 記載の電子ファイル管理装置。

【請求項 4】

上記保護電子ファイル出力手段は、

上記電子ファイルのアクセス要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、その保護電子ファイルを出力することを特徴とする請求項 1 記載の電子ファイル管理装置。

【請求項 5】

上記電子ファイル管理手段は、

上記電子ファイルの格納要求時に上記電子ファイルと上記保護電子ファイルとを受付けて、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納することを特徴とする請求項 1 記載の電子ファイル管理装置。

【請求項 6】

上記電子ファイルを暗号化する外部手段に対して、該電子ファイルと上記アクセス権限情報とを送信することによって上記保護電子ファイルを取得して、上記電子ファイル管理手段に提供する保護電子ファイル取得手段を有することを特徴とする請求項 1 記載の電子ファイル管理装置。

【請求項 7】

上記保護電子ファイルは、上記アクセス権限情報に基づいて上記電子ファイルを暗号化されたことを特徴とする請求項 1 乃至 6 記載の電子ファイル管理装置。

【請求項 8】

上記保護電子ファイル出力手段は、保護前の上記電子ファイルへのアクセス要求を受けると、保護前のドキュメントのアクセス権限があるか否かを判断し、その判断結果に基づいて、該アクセスを拒否することを特徴とする請求項 1 乃至 6 記載の電子ファイル管理装置。

【請求項 9】

上記電子ファイルにアクセス権限情報を付加して電子ファイル格納領域に格納する電子ファイル管理手順と、

上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能なプログラム。

【請求項 10】

アクセス要求に応じて、電子ファイルをアクセス権限情報に基づいて暗号化して保護した保護電子ファイルを提供するように該電子ファイルを管理し、

上記電子ファイルに対する処理要求に応じて上記保護電子ファイルを取得し、

上記保護電子ファイルが復号できた場合、上記アクセス権限情報に従って、復号された該保護電子ファイルに対して該処理を制御することを特徴とするファイルアクセス制御方法。

【請求項 1 1】

上記電子ファイルを識別する電子ファイル識別情報と、上記保護電子ファイルを復号する鍵と、上記アクセス制御情報とを管理し、

上記処理要求時に、該処理要求を行ったユーザを認証するユーザ認証情報、上記電子ファイル識別情報と、該処理タイプとを取得し、

ユーザ認証が成功した場合、上記アクセス権限情報に基づいて上記処理に対する許可又は不許可を判断し、その判断結果に基づいて、上記処理への許可時に指定される処理要件と、上記鍵とを取得し、

上記鍵によって上記保護電子ファイルを復号し、

上記処理要件に従って上記処理を制御することを特徴とするファイルアクセス制御方法。

【書類名】 明細書**【発明の名称】 電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法****【技術分野】****【0001】**

本発明は、セキュリティを必要とする技術文書などの電子ファイルを管理し、アクセス権限に応じて該電子ファイルに対するアクセス制御を行う電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法に関する。

【背景技術】**【0002】**

従来より、電子ファイルを管理する電子ファイル管理装置では、格納する電子ファイルに対して予めパスワードを登録させ、ユーザからのアクセス要求を受けると、そのユーザが登録されたパスワードを入力した場合にのみ、そのパスワードに対応する電子ファイルを表示装置や外部記憶装置に出力する。

【0003】

また、本出願人により先に出願されている（例えば、特許文献1）の「文書管理システム」は、電子化された文書を作成して登録し、承認されるとその文書を変換して印刷可能なPDFと印刷不可能なPDFとを作成し、利用権限に応じて閲覧できるファイルを制限するものである。

【特許文献1】 特開2001-142874号公報

【発明の開示】**【発明が解決しようとする課題】****【0004】**

しかしながら、従来の電子ファイル管理装置では、アクセス権限を認められたユーザが電子ファイルを取得した後、アクセス権限を認められていないユーザに取得した電子ファイルを渡すと、アクセス権限を認められていないユーザであってもその電子ファイルにアクセスできてしまうという問題があった。

【0005】

また、上述した特許文献1の文書管理システムは、電子化された文書を利用権限を認められていないユーザに対しても閲覧のみを許可しつつ印刷を不可能とする好適なものであるが、利用権限を認められているユーザが印刷可能なPDFを読み出した後、他の利用者にその印刷可能なPDFを渡してしまうと、本来印刷可能なPDFへのアクセス権限のない利用者でもPDFを印刷することができてしまっていた。

【0006】

本発明はこのような状況に鑑みてなされたものであり、オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアクセス権限に応じて適切に管理することができる電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を提供することである。

【課題を解決するための手段】**【0007】**

上記課題を解決するため、本発明は、請求項1に記載されるように、電子ファイルを格納する電子ファイル格納領域と、上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有するように構成される。

【0008】

このような電子ファイル管理装置では、アクセス権限情報を付加して電子ファイル（ドキュメント）を管理し、保護電子ファイル（保護ドキュメント）を出力するため、オリジナルの電子ファイルに対するセキュリティを向上することができる。

【0009】

また、本発明は、請求項2に記載されるように、上記電子ファイル管理手段は、上記電

子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納するように構成することができる。

【0010】

また、本発明は、請求項3に記載されるように、上記電子ファイル管理手段は、上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルを格納する代わりに、その保護電子ファイルを上記電子ファイル格納領域に格納するように構成することができる。

【0011】

また、本発明は、請求項4に記載されるように、上記保護電子ファイル出力手段は、上記電子ファイルのアクセス要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、その保護電子ファイルを出力するように構成することができる。

【0012】

また、本発明は、請求項5に記載されるように、上記電子ファイル管理手段は、上記電子ファイルの格納要求時に上記電子ファイルと上記保護電子ファイルとを受付けて、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納するように構成することができる。

【0013】

また、本発明は、請求項6に記載されるように、上記電子ファイルを暗号化する外部手段に対して、該電子ファイルと上記アクセス権限情報とを送信することによって上記保護電子ファイルを取得して、上記電子ファイル管理手段に提供する保護電子ファイル取得手段を有するように構成することができる。

【0014】

また、本発明は、請求項7に記載されるように、上記保護電子ファイルは、上記アクセス権限情報に基づいて上記電子ファイルを暗号化されるように構成することができる。

【0015】

また、本発明は、請求項8に記載されるように、上記保護電子ファイル出力手段は、保護前の上記電子ファイルへのアクセス要求を受けると、保護前のドキュメントのアクセス権限があるか否かを判断し、その判断結果に基づいて、該アクセスを拒否するように構成することができる。

【0016】

また、本発明は、請求項9に記載されるように、上記電子ファイルにアクセス権限情報を付加して電子ファイル格納領域に格納する電子ファイル管理手順と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手順とをコンピュータに実行させるように構成することができる。

【0017】

また、本発明は、請求項10に記載されるように、アクセス要求に応じて、電子ファイルをアクセス権限情報に基づいて暗号化して保護した保護電子ファイルを提供するように該電子ファイルを管理し、上記電子ファイルに対する処理要求に応じて上記保護電子ファイルを取得し、上記保護電子ファイルが復号できた場合、上記アクセス権限情報に従って、復号された該保護電子ファイルに対して該処理を制御するように構成することができる。

【0018】

また、本発明は、請求項11に記載されるように、上記電子ファイルを識別する電子ファイル識別情報と、上記保護電子ファイルを復号する鍵と、上記アクセス制御情報とを管理し、上記処理要求時に、該処理要求を行ったユーザを認証するユーザ認証情報、上記電子ファイル識別情報と、該処理タイプとを取得し、ユーザ認証が成功した場合、上記アクセス権限情報に基づいて上記処理に対する許可又は不許可を判断し、その判断結果に基づ

いて、上記処理への許可時に指定される処理要件と、上記鍵とを取得し、上記鍵によって上記保護電子ファイルを復号し、上記処理要件に従って上記処理を制御するように構成することができる。

【発明の効果】

【0019】

本願発明によれば、アクセス制限電子ファイルを、アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるように生成し、そのアクセス制限電子ファイルとオリジナル電子ファイルとを上記のアクセス権限情報に基づいて管理することにより、アクセス権限情報でアクセス権限を認められていないユーザに対して、アクセス制限電子ファイルをたとえ入手したとしてもアクセスできないようにすることができると共に、そのアクセス権限の管理を、管理者（アクセス権限の設定者）がアクセス権限情報を作成するだけで自動的に行うことができる。

【発明を実施するための最良の形態】

【0020】

以下、本発明の実施の形態を図面に基づいて説明する。

【0021】

先ず、本発明の実施形態としての電子ファイル管理装置における、各実施形態に共通する概要について説明する。

【0022】

本発明の実施形態としての電子ファイル管理装置は、コンピュータ装置本体と、ユーザが入力を行う入力装置と、ユーザに対して各種の情報を表示する表示装置とを備えて構成される。

【0023】

上記の入力装置は、例えばキーボードやマウスなどであり、表示装置は、例えばディスプレイなどである。

【0024】

コンピュータ装置本体は、オリジナルのドキュメント（Document；オリジナル電子ファイル）と保護ドキュメント（Protected Document；アクセス制限電子ファイル）との管理を行い、入力装置から操作を行うユーザに認められたアクセス権限に応じて上記の表示装置に出力する。

【0025】

コンピュータ装置本体からの出力先は上記の表示装置に限定されず、例えばプリンタをコンピュータ装置本体に接続することで、そのプリンタから印字（出力）することもできる。また、ユーザからのアクセス要求がFD（フロッピー（登録商標）ディスク）などのリムーバブルディスクといった情報記録媒体への保存である場合には、その情報記録媒体に保存することとしてよい。

【0026】

次に、本発明の第1の実施形態としての電子ファイル管理装置501について図1で説明する。図1は、本発明の第1の実施形態に係る電子ファイル管理装置を示す図である。

【0027】

図1（A）において、この第1の実施形態は、ドキュメント管理プログラム（Document Management Program）21を用いてドキュメント11（オリジナルのドキュメント；オリジナル電子ファイル）とACL（Access Control List；アクセス権限情報）12とを保存した際に、保護ドキュメント13を作成して、基本的にその保護ドキュメント13にのみアクセスさせるモデルである。

【0028】

第1の実施形態におけるコンピュータ装置本体によって制御される電子ファイル管理装置501は、管理者からドキュメント11とACL12とを受け取って管理するドキュメント管理プログラム（管理部）21と、そのドキュメント11とACL12とからアクセス制限をかけた保護ドキュメント13を生成するドキュメント保護プログラム（Document

Protection Program; アクセス制限部) 511と、電子ファイル(各種ドキュメント)やACL12などを格納するドキュメント管理DB(Document Management Database; 格納部)23とを有し、これらをHDDなどの記憶装置(不図示)に備えてなる。

【0029】

上記のACL12は、管理者によって設定されたドキュメント11へのアクセス権限であって、アクセスしてくるユーザによってドキュメント11へのアクセスを制限するための情報を含むものである。

【0030】

この第1の実施形態に係る電子ファイル管理装置501は、物理的には、各種のプログラムやデータなどを記憶する上記した記憶装置と、CPUなどの主制御装置とを備えて構成され、この主制御装置が記憶装置に格納されたプログラムにより処理を行うことで、この電子ファイル管理装置501は上述した管理部と、アクセス制限部と、格納部として機能する。

【0031】

すなわち、電子ファイル管理装置501は、上記の記憶部に記憶されたドキュメント管理プログラム21により主制御装置が処理を行うことで上記した管理部として機能し、上記の記憶装置に記憶されたドキュメント保護プログラム511により主制御装置が処理を行うことで、上記したアクセス制限装置として機能する。

【0032】

ACL12の構成例を図2に示す。この図2に示す例では、ACL12は、ユーザ名(User name)、アクセスタイプ(Access type)、許可情報(Permission)及び処理要件(Requirement)をパラメータとして構成される。

【0033】

すなわち、何らかのアクセス権限を認められたユーザのユーザ名(User name)に、そのユーザに認められたアクセス権限が、ユーザからの操作命令(Access type)ごとに関連付けられて構成されている。また、ユーザによる操作命令ごとに、許可(Allowed)と拒絶(Denied)とが定められている。

【0034】

なお、図1(A)及び図1(B)、図2に示す例では、ACL12には処理要件(Requirement)の項が入っているが、一般的なアクセス制御しきないのであれば、ACL12は処理要件(Requirement)の項がないものであってよい。

【0035】

このACL12は、ドキュメント11を作成した作成者や、電子ファイル管理装置501の管理者(管理者権限を持つユーザ)が作成し、そのドキュメント11に付与しておくこととする。電子ファイル管理装置501は、ドキュメント管理プログラム21により、入力装置によるユーザからの各操作命令に対し、このACL12に基づいて、上述した各種の出力を行う。

【0036】

次に、第1の実施形態にかかる電子ファイル管理装置501における電子ファイルの格納時の動作について、図1(A)、図3、図4、図5を参照して説明する。

【0037】

ドキュメント管理プログラム21がドキュメント11とACL12とを受け取って保存する際、ドキュメント管理プログラム21は受け取ったドキュメント11とACL12をドキュメント保護プログラム511に渡して保護ドキュメント13を受け取る。

【0038】

すなわち、ドキュメント保護プログラム511は、受け取ったACL12に設定されているアクセス権限の制限と同一の制限がドキュメント11にかけられるように、ドキュメント11から保護ドキュメント13を生成する。

【0039】

このドキュメント保護プログラム511による保護ドキュメント13の生成(暗号化)

とその復号化にかかるドキュメント保護・印刷システムの構成例を図 3 に示す。以下の説明では、この保護ドキュメント 1 3 の活用（復号化）用途を、プリンタ 5 0 3 により記録紙に印刷することとする。

【 0 0 4 0 】

この図 3 に示すドキュメント保護・印刷システム 5 0 0 1 は、電子ファイル管理装置 5 0 1、印刷用端末 5 0 2、プリンタ 5 0 3 及びアクセスコントロールサーバ 5 0 4 を有する。

【 0 0 4 1 】

電子ファイル管理装置 5 0 1 と印刷用端末 5 0 2 は、表示装置（例えば、LCD）、入力装置（例えば、キーボード）、外部記録装置（例えば、FDD、HDD）などを備えたコンピュータ端末を適用できる。なお、電子ファイル管理装置 5 0 1 にはドキュメント保護プログラム 5 1 1 が、印刷用端末 5 0 2 にはドキュメント印刷プログラム 5 2 1 がそれぞれ実装されている。

【 0 0 4 2 】

ドキュメント保護プログラム 5 1 1 は、ドキュメントファイルに電子ファイル管理装置 5 0 1 の管理者としてのユーザの入力操作に応じた印刷要件を設定するとともに、暗号化アルゴリズム（RC4、Triple DES、IDEA など）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【 0 0 4 3 】

なお、管理者の入力操作に応じてドキュメント保護プログラム 1 1 1 がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、BDP という）、機密印刷（Private Access：以下、PAC という）、電子透かし（Digital Watermark：以下、DWM という）の付加、バーコード付加（Embedding Barcode：以下、EBC という）、機密ラベルスタンプ（Security Label Stamp：以下、SLS という）などが挙げられる。

【 0 0 4 4 】

ドキュメント印刷プログラム 5 2 1 は、ユーザの入力操作に応じ、保護ドキュメント 1 3 を復号化するとともに、設定されている印刷要件に応じた印刷処理をプリンタ 5 0 3 に実行させる処理を行うプログラムである。

【 0 0 4 5 】

アクセスコントロールサーバ 5 0 4 は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム 5 2 1 からの要求に応じて ACL 1 2 を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。

【 0 0 4 6 】

アクセスコントロールサーバ 5 0 4 には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース 5 4 1 と、ユーザ各人ごとに設定された印刷要件を含む ACL 1 2 が登録される ACL データベース 5 4 2 とが接続されている。

【 0 0 4 7 】

上述のドキュメント保護・印刷システム 5 0 0 1 において、ドキュメント 1 1 と ACL 1 2 とを取得したドキュメント保護プログラム 5 1 1 は、上記の保護ドキュメント 1 3 を生成するに当たって、ドキュメントファイルごとに固有のドキュメント ID（Document ID）を生成し、復号に使用する暗号鍵（Key）と ACL 1 2 とをこれに関連づけてアクセスコントロールサーバ 5 0 4 へ送信し、登録する。

【 0 0 4 8 】

また、ドキュメント保護プログラム 5 1 1 は、図 5 に示すように、暗号鍵を用いてドキュメント 1 1 を暗号化し、その暗号化されたドキュメントファイル（暗号化ドキュメント）に対してドキュメント ID を付加して保護ドキュメント 1 3 を生成する。

【 0 0 4 9 】

こうして保護ドキュメント 1 3 が生成されると、ドキュメント管理プログラム 2 1 は、

受け取った保護ドキュメント 13 をドキュメント 11 及び ACL 12 と共に（関連づけて）ドキュメント管理 DB 23 に格納する。こうして、電子ファイル管理装置 501 は、ドキュメント 11 と保護ドキュメント 13 のペア（これをドキュメント・ペア（Document Pair）と呼ぶ）に ACL 12 を付与して（関連付けて）管理する。

【0050】

次に、第 1 の実施形態にかかる電子ファイル管理装置 501 が、管理しているドキュメント・ペアに対してユーザからアクセス要求を受けた時の動作について、図 1（B）、図 3 を参照して説明する。

【0051】

ドキュメント管理プログラム 21 は、ユーザからドキュメント・ペアに対するアクセス要求を受けるとユーザの認証を行う。この認証では、ドキュメント管理プログラム 21 は、ドキュメント・ペアに付与されている ACL 12 を参照して、アクセスしてきたユーザに参照権限がある、すなわち read 権限があると判断すると、保護ドキュメント 13 を返す。すなわち、電子ファイル管理装置 501 から上述のように表示装置などに出力する。

【0052】

上記の認証で、アクセスしてきたユーザに参照権限がない、すなわち read 権限が認められていないとドキュメント管理プログラム 21 が判断すると、表示装置にその旨を表示する。

【0053】

この出力された保護ドキュメント 13 の復号化について、上述した図 3 に示すドキュメント保護・印刷システム 5001 の例により説明する。

【0054】

なお、図 3 に示すドキュメント保護・印刷システム 5001 の例では、ドキュメントファイルを印刷や参照しようとするユーザに対する上述の電子ファイル管理装置 501 からの出力として、管理者により FD などの情報記録媒体による受け渡しを行う場合と、通信網により印刷用端末 502 へ送信する場合とを示している。

【0055】

ユーザがドキュメント 11 を印刷しようとする場合には、印刷用端末 502 に保護ドキュメント 13 を実装する。例えば、上述のように電子ファイル管理装置 501 から情報記録媒体に出力（記録）された保護ドキュメント 13 を外部記録装置を用いて印刷用端末 502 に読み取らせても良いし、印刷用端末 502 が電子ファイル管理装置 501 と通信可能である場合には、通信網を介して電子ファイル管理装置 501 から保護ドキュメント 13 を印刷用端末 502 に出力させるようにしてもよい。

【0056】

ユーザが、印刷用端末 502 の入力装置を介してドキュメント印刷プログラム 521 に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム 521 は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム 521 は、印刷用端末 502 の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【0057】

ドキュメント印刷プログラム 521 は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ 504 へ送信して、ユーザ認証を要求する。

【0058】

アクセスコントロールサーバ 504 は、ドキュメント印刷プログラム 521 から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【0059】

ユーザを特定すると、アクセスコントロールサーバ 504 は、ACL データベース 542 を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかといった

、アクセス権限の制限の情報を取得する。

【0060】

ユーザにドキュメントファイル（保護ドキュメント13）を印刷する権限がある場合、アクセスコントロールサーバ504は、その旨を示す認証情報とともに、保護ドキュメント13を復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とを印刷用端末502を介してドキュメント印刷プログラム521に通知する。

【0061】

アクセスコントロールサーバ504から認証情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム521は、暗号鍵を用いて保護ドキュメント13を復号化してドキュメント11に復元する。

【0062】

そしてドキュメント印刷プログラム521は、印刷要件を満たすようにプリンタ503に印刷処理を実行させる。例えば、ドキュメントファイルにBDP（地紋印刷）が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋を印刷する。

【0063】

以上により、ドキュメントファイルを印刷する際に、管理者がユーザ各人に対して設定した印刷要件、すなわちACL12としてユーザ各人に対して設定したアクセス権限の制限を強制することが可能となる。

【0064】

次に、第1の実施形態に係るドキュメント管理プログラム21によって実現される機能構成について図4で説明する。図4は、第1の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアントc1及びc2は、同一クライアントであってもよい。

【0065】

図4において、ドキュメント管理プログラム21によって、少なくとも、ドキュメント保管要求受付部21aと、ドキュメント保管部21b保護ドキュメント取得部21cと、ドキュメント参照要求受付部21dと、ドキュメント取得部21eとが機能として構成される。

【0066】

ドキュメント保管要求受付部21aは、ドキュメント11の保管を要求するクライアントc1から、ドキュメント保管要求とともにドキュメント11とACL12を受け取ると、受け取ったドキュメント11とACL12をドキュメント保管部21bに渡す。

【0067】

ドキュメント保管部21bは受け取ったドキュメント11をドキュメント管理DB23に格納し、受け取ったACL12をその格納したドキュメント11のACL12として設定する。ドキュメント保管部21bは格納したドキュメント11の識別子（ドキュメントID）を返す。

【0068】

ドキュメント保管要求受付部21aは、ドキュメント保管部21bからドキュメントIDを受け取ると、ドキュメント11、ACL12、ドキュメントIDを保護ドキュメント取得部21cに渡す。保護ドキュメント取得部21cはドキュメント11とACL12をドキュメント保護プログラム511に渡して保護ドキュメント13を取得し、ドキュメントIDと保護ドキュメント13をドキュメント保管部21bに渡す。

【0069】

ドキュメント保管部21bはドキュメントIDで指定されたドキュメント11に関連付けてその保護ドキュメント13をドキュメント管理DB23に格納する。

【0070】

ドキュメント保管要求受付部21aは、ドキュメント保管要求をしたクライアントc1にドキュメントIDを返す。返すタイミングは、ドキュメント11を保管してすぐでも良いし、保護ドキュメント13が格納されたことを確認した後でも良い。

【0071】

また、ドキュメント参照要求受付部 21d は、ドキュメント 11 の参照を要求するクライアント c2 から、ドキュメント参照要求とともにドキュメント ID を受け取ると、受け取ったドキュメント ID をドキュメント取得部 21e に渡す。

【0072】

ドキュメント取得部 21e は、受け取ったドキュメント ID をもとにドキュメント管理 DB 23 から該当するドキュメント 11 の ACL 12 を確認し、参照権限のあるユーザからの要求であれば、そのドキュメント 11 とともに格納されている保護ドキュメント 13 をドキュメント管理 DB 23 から取得し、ドキュメント参照要求受付部 21d に返す。

【0073】

ドキュメント参照要求受付部 21d は、ドキュメント参照要求をしたクライアント c2 に受け取った保護ドキュメント 13 を返す。ドキュメント参照要求をしてクライアント c2 を使用しているユーザに参照権限がない場合にはエラーを返す。その一方で、ユーザにオリジナルを参照する特別な権限が与えられている場合には、保護ドキュメント 13 を返すのではなく、オリジナルのドキュメント 11 を返すようにしても良い。

【0074】

次に、ドキュメント 11 から保護ドキュメント 13 を生成する際のドキュメント保護プログラム 511 及びアクセスコントロールサーバ 504 の動作、及び保護ドキュメント 13 をドキュメント 11 に復元して印刷する際のドキュメント印刷プログラム 521 及びアクセスコントロールサーバ 504 の動作についてさらに詳しく説明する。

【0075】

ドキュメント保護プログラム 511 が保護ドキュメント 13 を生成する際の動作を図で説明する。図 5 は、ドキュメント保護プログラムの動作を示す図である。

【0076】

図 5 において、ドキュメント保護プログラム 511 は、電子ファイル管理装置 501 の入力装置における管理者の入力操作によってドキュメントファイルと ACL 12 とを取得すると、ドキュメントファイルの暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム 511 は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。

【0077】

さらにドキュメント保護プログラム 511 は、ドキュメントファイルごとに固有のドキュメント ID を暗号化ドキュメントに添付して保護ドキュメント 13 を生成する。

【0078】

保護ドキュメント 13 を生成した後、ドキュメント保護プログラム 511 は電子ファイル管理装置 501 の通信機能を用いて、暗号鍵と ACL 12 とドキュメント ID とをアクセスコントロールサーバ 504 へ送信し、これらの登録をアクセスコントロールサーバ 504 に要求する。

【0079】

暗号鍵と ACL 12 とドキュメント ID とをドキュメント保護プログラム 511 から受け渡されたアクセスコントロールサーバ 504 は、図 6 に示すように、これらを関連づけて一つのレコードとして ACL データベース 542 に記録保持する。図 6 は、ACL データベースに記録される情報の構造例を示す図である。図 6 において、ACL データベース 542 は、ドキュメント ID (Document ID) ごとに、暗号鍵 (Key) と、ACL 12 とを管理する。

【0080】

なお、上記の例においてはドキュメント ID の生成や暗号鍵の生成をドキュメント保護プログラム 511 が行う場合を示したが、これらの処理はアクセスコントロールサーバ 504 やドキュメント ID の生成や暗号鍵の生成を行う別のサーバ (不図示) などで行っても良い。

【0081】

また、電子ファイル管理装置 501 とアクセスコントロールサーバ 504 との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、SSL (Secure Socket Layer) を用いて通信を行えばよい。

【0082】

ドキュメント保護プログラム 511 がアクセスコントロールサーバ 503 と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Java (登録商標) RMI (Remote Method Invocation) や SOAP (Simple Object Access Protocol) をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ 504 は、例えば register (String docId, byte[] key, byte[] acl) のようなメソッドを実装するようにしてもよい。SOAP であれば、HTTP の上で SOAP プロトコルをやりとりし、RMI であれば SSL ベースの SocketFactory を用いて RMI を実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【0083】

次に、ドキュメント印刷プログラム 521 が保護ドキュメント 13 を印刷する際の動作について図 7 で説明する。

【0084】

図 7 は、ドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【0085】

図 7 において、ドキュメント印刷プログラム 521 は、印刷用端末 502 の入力装置におけるユーザの入力操作によって保護ドキュメント 13 とユーザ名とパスワードとを取得すると、保護ドキュメント 13 に添付されているドキュメント ID を取得する (ステップ S511)。

【0086】

そして、ユーザ名とパスワードとドキュメント ID とアクセスタイプ (ユーザが要求する処理を示す情報。ここでは、保護ドキュメント 13 を印刷しようとするので “print” となる。) とをアクセスコントロールサーバ 504 へ送信して、アクセス権限があるか否かのチェックを要求する (ステップ S512)。

【0087】

なお、図 8 は、アクセスコントロールへの SOAP による問い合わせの例を示す図であり、ユーザ名 (userId) とドキュメント ID (docId) とアクセスタイプ (accessType) とを渡してアクセスが許可されているかを問い合わせる SOAP メッセージ (isAllowed) を送付し、その結果 (isAllowedResponse) を受け取っている例である。結果には、許可されているということ (allowed が true) と要件 (requirements) とが含まれている。

【0088】

アクセスコントロールサーバ 504 は、ドキュメント印刷プログラム 521 からユーザ名とパスワードとドキュメント ID とアクセスタイプとを取得すると、ユーザデータベース 541 に登録されている情報を参照し (ステップ S513)、ユーザ認証を行う (ステップ S514)。

【0089】

換言すると、アクセスコントロールサーバ 504 は、ユーザデータベース 541 に登録されている情報を参照し、ドキュメント印刷プログラム 521 から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース 541 に組として登録されているか否かを判断する。

【0090】

ユーザ認証に失敗した場合 (換言すると、ドキュメント印刷プログラム 521 から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース 541 に登録されていない場合)、アクセスコントロールサーバ 504 は、許可情報 (ユーザが要求する処理を許可するか否かを示す情報) を「不許可」として印刷用端末 502 へ

送信し、ドキュメント印刷プログラム 5 2 1 へ受け渡す（ステップ S 5 1 5）。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム 5 2 1 へ受け渡すようにしてもよい（ステップ S 5 1 6）。

【0 0 9 1】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ 5 0 4 は、ACL データベース 5 4 2 に格納されているレコードのうち、ドキュメント印刷プログラム 5 2 1 から取得した情報に含まれるドキュメント ID に関するレコードを読み出す（ステップ S 5 1 7）。

【0 0 9 2】

アクセスコントロールサーバ 5 0 4 は、読み出したレコードに含まれる ACL 1 2 を取得し、ドキュメント印刷プログラム 5 2 1 から取得したユーザ名及びアクセスタイプに基づいて、ACL 1 2 から許可情報および印刷要件を取得する（ステップ S 5 1 8）。

【0 0 9 3】

換言すると、アクセスコントロールサーバ 5 0 4 は、ユーザ名とアクセスタイプとに基づいて、予め ACL 1 2 に設定されている許可情報と印刷要件とを取得する（ステップ S 5 1 9）。

【0 0 9 4】

ACL 1 2 から取得した許可情報が「許可」を示すか否かを判断する（ステップ S 5 2 0）。ACL 1 2 から取得した許可情報が「許可」である場合、アクセスコントロールサーバ 5 0 4 は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともに印刷用端末 5 0 2 へ送信してドキュメント印刷プログラム 5 2 1 に受け渡す（ステップ S 5 2 1）。

【0 0 9 5】

一方、ACL 1 2 から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ 5 0 4 は、許可情報のみを印刷用端末 5 0 2 へ送信してドキュメント印刷プログラム 5 2 1 に受け渡す。

【0 0 9 6】

アクセスコントロールサーバ 5 0 4 から許可情報を受け渡されたドキュメント印刷プログラム 5 2 1 は、取得した許可情報を参照し、「不許可」である場合には、印刷用端末 5 0 2 の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する（ステップ S 5 2 2）。

【0 0 9 7】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号してドキュメントファイルに復元する（ステップ S 5 2 3）。

【0 0 9 8】

また、ドキュメント印刷プログラム 5 2 1 は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、PAC が指定されていれば機密印刷モードに設定する）、プリンタ 5 0 3 にドキュメントの印刷処理を実行させる。

【0 0 9 9】

なお、必要があれば、印刷用端末 5 0 2 の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【0 1 0 0】

アクセスコントロールサーバ 5 0 4 から取得した印刷要件を満足する印刷をプリンタ 5 0 3 では実行できない場合、換言すると、プリンタ 5 0 3 が ACL 1 2 に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【0 1 0 1】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、アクセスコントロールサーバ 5 0 4 側でドキュメントファ

イルに対するアクセス権限を判断するシステム構成においては、ACLデータベース542に登録されているACL12の内容を電子ファイル管理装置501やアクセスコントロールサーバ504における入力操作によって変更できるようにてもよく、この場合には、保護ドキュメント13を配布した後で印刷要件を変更したりすることが可能となる。

【0102】

例えば、既に配布した保護ドキュメント13に対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【0103】

なお、本実施形態を用いる図3に示すドキュメント保護・印刷システム5001が上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム521に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメント13を復号することも可能ではある。この場合は、ACL12として設定されている印刷要件を強制されることなく、保護ドキュメント13を印刷できてしまうこととなる。

【0104】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム511の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

【0105】

この場合は、ドキュメント印刷プログラム521にも同一の秘密鍵を埋め込んでおくことで、管理者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム521のみが、保護ドキュメント13を復号して印刷することが可能となる。

【0106】

また、図3を用いて上述したドキュメント保護・印刷システム5001においては、ドキュメント印刷プログラム521は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム521は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat（登録商標）のプラグインとしてこの機能を実現することが可能である。

【0107】

なお、この第1の実施形態としての電子ファイル管理装置501では、上述した図2に示すACL12の例には記載していないが、ACL12のAccess typeとして例えばGetOriginal（オリジナル電子ファイルへのアクセス権限）を定義し、そのGetOriginalのアクセス権限を認められているユーザがドキュメント・ペアにアクセスした場合には、ドキュメント管理プログラム511は保護ドキュメント13を返すのではなく、ドキュメント11を返すようにしてもよい。

【0108】

すなわち、電子ファイル管理装置501がGetOriginalを定義されたACL12に基づいてユーザ認証を行い、アクセスしたユーザにGetOriginalのアクセス権限が認められている場合にはドキュメント11を電子ファイル管理装置501から上述のように出力するようにしてもよい。

【0109】

また、ACL12にオリジナル電子ファイルであるドキュメント11へのアクセス権限を定義しなくても、特別なユーザのみ（例えば保存したユーザのみ）がドキュメント11へのアクセス権限を認められることとしてもよい。すなわち、ドキュメント管理プログラム511が、予め設定された特別なユーザのみにドキュメント11へのアクセス権限を認めることとしてもよい。

【0110】

本実施形態によれば、ドキュメント管理プログラム511により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置501から出力された）ドキュメント（ポータブルドキュメント）への

アクセス制御とを統一することができる。

【0111】

また、管理者はACL12としてアクセス権限の制限を設定し、ドキュメント11とACL12とをドキュメント管理プログラム511に渡すよう電子ファイル管理装置501を入力装置により操作するだけで、設定したアクセス権限に応じて保護ドキュメント13をユーザに渡すよう電子ファイル管理装置501に管理させることができる。

【0112】

すなわち、管理者がACL12としてアクセス権限の制限を一度設定するだけで、電子ファイル管理装置501は、表示装置や外部記録装置などへの出力をそのアクセス権限の制限により管理することができる。

【0113】

さらに、上述のようにオリジナル電子ファイルへのアクセス権限を定義することで、電子ファイル管理装置501は、上記したアクセス権限の制限による管理をドキュメント11と保護ドキュメント13とに対して行うことができる。すなわち、電子ファイル管理装置501は、ACL12として設定されたアクセス権限に応じてドキュメント11又は／及び保護ドキュメント13を出力するよう管理することができる。

【0114】

図1(A)及び図1(B)に示す電子ファイル管理装置501の他の例を図9で説明する。図9は、本発明の第1の実施形態に係る電子ファイル管理装置の他の例を示す図である。図1(A)及び図1(B)に示す電子ファイル管理装置501において、図9(A)及び図9(B)に示すようにオリジナルのドキュメント11-2のみを管理することもできる。

【0115】

図9(A)において、ドキュメント管理プログラム21がドキュメント11-2のみを受け取って保存する際、ドキュメント管理プログラム21は、受け取ったドキュメント11-2を、直接ドキュメント管理DB23に格納する。また、図9(B)において、ドキュメント管理プログラム21は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント11-2に対するアクセス要求に対してドキュメント11-2を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ACL12との比較によるユーザのread権限の判断は行わない。

【0116】

次に、本発明の第2の実施形態としての電子ファイル管理装置505について、図10を参照して説明する。図10は、本発明の第2の実施形態に係る電子ファイル管理装置を示す図である。

【0117】

この第2の実施形態は、ドキュメント管理プログラム21が、第1の実施形態でドキュメント管理DB23にドキュメント11と保護ドキュメント13(ドキュメント・ペア)をACL12に関連付けて格納していたのに替えて、保護ドキュメント13を格納し、ドキュメント11を破棄するものである。

【0118】

すなわち、第1の実施形態のようにドキュメント11を残しておくと、そのドキュメント11にアクセス可能なユーザがプロテクトされていないドキュメント11を流通させてしまう可能性がある。そのようなことが心配される環境では、この第2の実施形態とすることで保護ドキュメント13を好適に管理することができる。

【0119】

この第2の実施形態の電子ファイル管理装置505は、物理的な構成は上述した第1の実施形態と同様であり、図10に示すように、ドキュメント管理プログラム51と、ドキュメント保護プログラム22と、ドキュメント管理DB23と、をHDDなどの記憶部(不図示)に備えてなる。

【0120】

上述した第1の実施形態と同様のものについては同じ符号とし、説明を省略する。

【0121】

また、ドキュメント保護プログラム22がドキュメント11から保護ドキュメント13を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント13を復号してプリンタにより印刷する際のシステムや動作も、図3、図5から図8を用いて上述したものと同様であってよい。

【0122】

この第2の実施形態にかかる電子ファイル管理装置505における電子ファイル格納時の動作について、図10(A)を参照して説明する。

【0123】

ドキュメント管理プログラム51にドキュメント11とACL12を渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム51は、受け取ったドキュメント11とACL12とをドキュメント保護プログラム511に渡して保護ドキュメント13を受け取る。すなわち、上述のようにドキュメント保護プログラム511に保護ドキュメント13を生成させる。

【0124】

生成された保護ドキュメント13を受け取ると、ドキュメント管理プログラム51は、受け取った保護ドキュメント13をドキュメント管理DB23に格納し、ドキュメント11とACL12とは破棄する。

【0125】

この第2の実施形態にかかる電子ファイル管理装置505が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図10(B)を参照して説明する。

【0126】

ドキュメント管理プログラム51はドキュメントに対するアクセス要求を受けると、ドキュメント管理DB23に格納している保護ドキュメント13を返す。すなわち、電子ファイル管理装置505から上述のように表示装置などに出力する。

【0127】

本実施形態では、ドキュメント11は破棄され、保護ドキュメント13はユーザによって読み出された後、ACL12に従ってアクセス制御されるため、ドキュメント管理プログラム51でアクセス制御を行う必要はない。

【0128】

しかし、保護ドキュメント13を取得されると暗号を解読されて内容にアクセスされる可能性もあるため、その可能性を少しでも減らすために、上述した第1の実施形態と同様に、ドキュメント管理プログラム51が保護ドキュメント13をドキュメント管理DB23に格納する際、保護ドキュメント13にACL12を関連付けて格納（ACL12を付与して管理）し、そのACL12に基づいてアクセス制御を行うようにしてもよい。すなわち、上記したドキュメント11を破棄する際に、ドキュメント管理プログラム51はACL12を破棄せず、保護ドキュメント13に関連付けてドキュメント管理DB23に格納することとしてもよい。

【0129】

このようにアクセス制御を行うことで、ドキュメント管理プログラム51により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置505から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【0130】

本実施形態によれば、暗号化されていないドキュメント11を破棄することにより、管理しているドキュメントをより確実に保護することができる。

【0131】

図10(A)及び図10(B)に示す電子ファイル管理装置505の他の例を図11で

説明する。図11は、本発明の第2の実施形態に係る電子ファイル管理装置の他の例を示す図である。図10(A)及び図10(B)に示す電子ファイル管理装置505-2において、図11(A)及び図11(B)に示すようにオリジナルのドキュメント11-2のみを管理することもできる。

【0132】

図11(A)において、ドキュメント管理プログラム51がドキュメント11-2のみを受け取って保存する際、ドキュメント管理プログラム51は、受け取ったドキュメント11-2を、直接ドキュメント管理DB23に格納する。また、図11(B)において、ドキュメント管理プログラム51は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント11-2に対するアクセス要求に対してドキュメント11-2を表示装置などに出力する。

【0133】

次に、第2の実施形態に係るドキュメント管理プログラム51によって実現される機能構成について図12で説明する。図12は、第2の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【0134】

図12において、図4に示すドキュメント管理プログラム21とは異なり、こちらはオリジナルのドキュメント11はドキュメント管理DB13で管理しない実施例である。ドキュメント管理プログラム51によって、少なくとも、ドキュメント保管要求受付部51aと、ドキュメント保管部51bと、保護ドキュメント取得部51cと、ドキュメント参照要求受付部51dと、ドキュメント取得部51eとが機能として構成される。

【0135】

ドキュメント保管要求受付部51aは、ドキュメント保管部51bにドキュメント11を渡さず、ACL12のみを渡してドキュメントIDを取得しておく。図12に示すドキュメント管理プログラム51では、ACL12のみが設定された空のドキュメントエリア13-2をドキュメント管理DB23に作成しておいて、後からその空のドキュメントエリア13-2に保護ドキュメント13を格納する例を示している。

【0136】

保護ドキュメント取得部51cと、ドキュメント参照要求受付部51dと、ドキュメント取得部51eとは、図4に示す保護ドキュメント取得部21cと、ドキュメント参照要求受付部21dと、ドキュメント取得部21eと同様の動作を行うため、その説明を省略する。

【0137】

もちろん、空のドキュメントエリア13-2を先に作らず、保護ドキュメント13を作成してからドキュメントエリア13-2を確保して格納するようにしても良い。

【0138】

この例の場合、ドキュメント管理プログラム51は保護ドキュメント13のみを管理するプログラムとなるため、ドキュメント保護プログラム511と同じコンピュータで稼働させるのが現実的である。

【0139】

次に、本発明の第3の実施形態としての電子ファイル管理装置61について、図13で説明する。

【0140】

この第3の実施形態は、ドキュメント管理プログラムが、第1の実施形態でドキュメント保護プログラム511に保護ドキュメント13を生成させて、ドキュメント管理DB23にドキュメント11と保護ドキュメント13(ドキュメント・ペア)をACL12に関連付けて格納していたのに替えて、ドキュメント11をACL12に関連付けてそのまま格納し、ユーザからアクセス要求を受けた際にドキュメント保護プログラム511に保護ドキュメント13を生成させて上述のように出力するものである。

【0141】

すなわち、第1の実施形態のような管理を行う場合、保護ドキュメント13を保存しておく分だけディスク領域を多く必要とすることになる。そこで、この第3の実施形態は、ドキュメントへのアクセスがユーザから要求されたときに動的に保護ドキュメント13を作成することで、余分なディスク領域を使用せずにすむ好適な管理を行うことができる。

【0142】

図13は、第3の実施形態の電子ファイル管理装置の例を示す図である。図13において、この第3の実施形態の電子ファイル管理装置506は、物理的な構成は上述した第1の実施形態と同様であり、ドキュメント管理プログラム61と、ドキュメント保護プログラム511と、ドキュメント管理DB23と、をHDDなどの記憶部（不図示）に備えている。上述した第1の実施形態と同様のものについては同じ符号とし、説明を省略する。

【0143】

また、ドキュメント保護プログラム511がドキュメント11から保護ドキュメント13を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント13を復号してプリンタ503により印刷する際のシステムや動作も、図3、図5から図8を用いて上述したものと同様であってよい。

【0144】

この第3の実施形態にかかる電子ファイル管理装置506における電子ファイル格納時の動作について、図13（A）を参照して説明する。

【0145】

ドキュメント管理プログラム61にドキュメント11とACL12を渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム61は、受け取ったドキュメント11にACL12を付与してドキュメント管理DB23に格納する。

【0146】

この第3の実施形態にかかる電子ファイル管理装置506が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図8（B）を参照して説明する。

【0147】

ドキュメント管理プログラム61は、ドキュメントに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント11に付与されているACL12に基づいてそのユーザにアクセス権限があるかどうか確認する。そのユーザにアクセス権限がある場合、ドキュメント管理プログラム61は、ドキュメント管理DB23から指定されたドキュメント11とACL12を取り出し、ドキュメント保護プログラム511に渡して保護ドキュメント13を上述のように生成させて受け取り、その生成された保護ドキュメント13をドキュメント管理プログラム61への呼び出し側へ返す。すなわち、電子ファイル管理装置506から上述のように表示装置などに出力する。

【0148】

なお、この第3の実施形態においても、上述した第1の実施形態と同様に、ACL12のAccess typeとして例えばGetOriginal（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置506がユーザ認証を行うことで、GetOriginalのアクセス権限が認められているユーザに対して、保護ドキュメント13ではなく、ドキュメント11を返す（要求に応じて出力する）ようにしてもよい。

【0149】

図13（A）及び図13（B）に示す電子ファイル管理装置506の他の例を図14で説明する。図14は、本発明の第3の実施形態に係る電子ファイル管理装置の他の例を示す図である。図14（A）及び図14（B）に示す電子ファイル管理装置506-2において、オリジナルのドキュメント11-2のみを管理するようにすることもできる。

【0150】

図14（A）において、ドキュメント管理プログラム61がドキュメント11-2のみを受け取って保存する際、ドキュメント管理プログラム61は、受け取ったドキュメント

1 1 - 2 を、直接ドキュメント管理 DB 2 3 に格納する。また、図 1 4 (B) において、ドキュメント管理プログラム 6 1 は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント 1 1 - 2 に対するアクセス要求に対してドキュメント 1 1 - 2 を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ACL 1 2 との比較によるユーザの read 権限の判断は行わない。

【0 1 5 1】

次に、第 3 の実施形態に係るドキュメント管理プログラム 6 1 によって実現される機能構成について図 1 5 で説明する。図 1 5 は、第 3 の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアント c 1 及び c 2 は、同一クライアントであってもよい。

【0 1 5 2】

図 1 5 において、ドキュメント管理プログラム 6 1 は、予め保護ドキュメントを 1 3 生成しておくのではなく、ユーザからのアクセス要求があったときに動的に保護ドキュメント 1 3 を生成する。ドキュメント管理プログラム 6 1 によって、少なくとも、ドキュメント保管要求受付部 6 1 a と、ドキュメント保管部 6 1 b と、保護ドキュメント取得部 6 1 c と、ドキュメント参照要求受付部 6 1 d と、ドキュメント取得部 6 1 e とが機能として構成される。

【0 1 5 3】

ドキュメント保管要求受付部 6 1 a は、ドキュメント保管要求を行ったクライアント c 1 からドキュメント保管要求と共に、ドキュメント 1 3、ACL 1 2 を受け取ると、そのドキュメント 1 1 と ACL 1 3 をドキュメント保管部 6 1 b に渡す。

【0 1 5 4】

ドキュメント保管部 6 1 b は、受け取ったドキュメント 1 1 をドキュメント管理 DB 2 3 に格納し、受け取った ACL 1 2 を格納したドキュメント 1 1 に設定して、そのドキュメント 1 1 を識別するドキュメント ID を返す。

【0 1 5 5】

そして、ドキュメント保管要求受付部 6 1 a は、ドキュメント ID をドキュメント保管要求を行ったクライアント c 1 に返す。

【0 1 5 6】

ドキュメント参照要求受付部 6 1 d は、ドキュメント参照要求を行ったクライアント c 1 からドキュメント参照要求とともにドキュメント ID を受け取ると、ドキュメント取得部 6 1 e にドキュメント ID を渡す。

【0 1 5 7】

ドキュメント取得部 6 1 e は、受け取ったドキュメント ID に該当するドキュメント 1 1 に付与されている ACL 1 2 を参照し、アクセスを要求しているユーザに参照する権限があるかどうかを確認する。権限がある場合には、ドキュメント ID に該当するドキュメント 1 1 をドキュメント管理 DB 2 3 から取得する。取得したドキュメント 1 1 と ACL 1 2 を保護ドキュメント取得部 6 1 c に渡す。

【0 1 5 8】

保護ドキュメント取得部 6 1 c は受け取ったドキュメント 1 1 と ACL 1 2 をドキュメント保護プログラム 5 1 1 に渡して保護ドキュメント 1 3 を取得して保護ドキュメント取得部 6 1 c に返す。

【0 1 5 9】

保護ドキュメント取得部 6 1 c は、受け取った保護ドキュメント 1 3 をドキュメント取得部 6 1 c に渡す。ドキュメント取得部 6 1 e は、受け取った保護ドキュメント 1 3 をドキュメント参照要求受付部 6 1 d に渡す。

【0 1 6 0】

ドキュメント参照要求受付部 6 1 d は、受け取った保護ドキュメント 1 3 をドキュメント参照要求を行ったクライアント c 2 に返す。

【0 1 6 1】

参照する権限がないユーザは、結局、保護ドキュメント 13 にアクセスできないのだから権限を確認せずに誰にでも保護ドキュメント 13 を取得して渡すようにしても良い。ただし、暗号化されているとはいえ、保護ドキュメント 13 を渡してしまうことは暗号を力づくで解読するチャンスを与えることになるため、上記のようにアクセス権のないユーザには保護ドキュメントすらアクセスさせないようにするのは意味がある。

【0162】

本実施形態によれば、ドキュメント管理プログラム 61 により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（装置本体 6a から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【0163】

また、使用するディスク領域を保護ドキュメント 13 の分だけ小さくすることができるため、ディスク容量が比較的小さい場合であっても好適な管理ができるようになる。

【0164】

次に、本発明の第 4 の実施形態としての電子ファイル管理装置 507 について、図 16 を参照して説明する。図 16 は、本発明の第 4 の実施形態に係る電子ファイル管理装置を示す図である。

【0165】

この第 4 の実施形態における電子ファイル管理装置 507 では、ドキュメント管理プログラム 71 が、第 1 の実施形態でドキュメント保護プログラム 511 に保護ドキュメント 13 を生成させて、ドキュメント管理 DB 23 にドキュメント 11 と保護ドキュメント 13（ドキュメント・ペア）を ACL 12 に関連付けて格納していたのに対し、予めドキュメント保護プログラム 511 に保護ドキュメント 13 を生成させて保存し、ドキュメント管理 DB 23 にドキュメント 11 と保護ドキュメント 13（ドキュメント・ペア）とを ACL 12 に関連付けて格納する。

【0166】

すなわち、電子ファイル管理装置 507 が内部でドキュメント保護プログラム 511 を実行するのは、処理のパフォーマンス面から難しくなることも考えられる。そのような場合であっても、あらかじめドキュメント保護プログラム 511 によってプロテクトした保護ドキュメント 13 をドキュメント管理プログラム 71 により保存することで、ドキュメント 11 と保護ドキュメント 13 を適切に管理することができるようにするものである。

【0167】

この第 4 の実施形態の電子ファイル管理装置 507 は、物理的な構成は上述した第 1 の実施形態と同様であり、図 16 に示すように、ドキュメント管理プログラム 71 と、ドキュメント保護プログラム 511 と、ドキュメント管理 DB 23 と、を HDD などの記憶部（不図示）に備えてなる。

【0168】

上述した第 1 の実施形態と同様のものについては同じ符号とし、説明を省略する。

【0169】

また、ドキュメント保護プログラム 22 がドキュメント 11 から保護ドキュメント 13 を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント 13 を復号してプリンタにより印刷する際のシステムや動作も、図 3、図 5 から図 8 を用いて上述したものと同様であってよい。

【0170】

この第 4 の実施形態にかかる電子ファイル管理装置 507 における電子ファイル格納時の動作について、図 16（A）を参照して説明する。

【0171】

ユーザはまず、ドキュメント保護プログラム 511 にドキュメント 11 と ACL 12 とを渡して保護ドキュメント 13 を生成させる。

【0172】

ドキュメント管理プログラム 71 にドキュメント 11 と ACL 12 と生成された保護ドキュメント 13 とを渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム 71 は、受け取ったドキュメント 11 と保護ドキュメント 13（ドキュメント・ペア）をドキュメント管理 DB 23 に格納し、受け取った ACL 12 を付与して管理する。

【0173】

この第 4 の実施形態にかかる電子ファイル管理装置 507 が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図 16（B）を参照して説明する。

【0174】

ドキュメント管理プログラム 71 は、ドキュメント・ペアに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント・ペアに付与されている ACL 12 に基づいてアクセス権限があるかどうかを確認する。アクセス権限がある場合には、ドキュメント管理 DB 23 に格納している保護ドキュメント 13 を返す。すなわち、電子ファイル管理装置 507 から上述のように表示装置などに出力する。

【0175】

なお、この第 4 の実施形態においても、上述した第 1 の実施形態と同様に、ACL 12 の Access type として例えば Get Original（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置 7 がユーザ認証を行うことで、Get Original のアクセス権限が認められているユーザに対して、保護ドキュメント 13 ではなく、ドキュメント 11 を返す（要求に応じて出力する）ようにしてもよい。

【0176】

また、この第 4 の実施形態では、ドキュメント保護プログラム 511 は電子ファイル管理装置 507 に替えて、他の装置に実装されていてもよい。この場合、ドキュメント保護プログラム 511 が実装された装置でドキュメント 11 から保護ドキュメント 13 を生成し、その生成を行った装置からネットワークや情報記録媒体などにより電子ファイル管理装置 507 にドキュメント 11 と、保護ドキュメント 13 と、ACL 12 とを渡すこととなる。

【0177】

また、ドキュメント管理プログラム 71 への保存の際にドキュメント 11 と保護ドキュメント 13 を両方渡すのではなく、保護ドキュメント 13 のみを渡してドキュメント 11 を破棄するようにしてもよい。この場合、ユーザからのアクセス要求を受けた際には、上述した第 2 の実施形態と同様の動作となる。

【0178】

本実施形態によれば、ドキュメント管理プログラム 71 により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置 507 から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【0179】

また、ドキュメント保護プログラム 511 による保護ドキュメント 13 の生成を、電子ファイル管理装置 507 における他の重い処理と同時にしないように行うことができるため、電子ファイル管理装置 507 の処理能力が比較的低い場合であっても保護ドキュメント 13 の生成などの処理を適切に行うことができる。

【0180】

また、ドキュメント保護プログラム 511 による保護ドキュメント 13 の生成を他の装置で行うことにより、生成などの処理にかかる負担を効果的に分散させることができる。このことにより、電子ファイル管理装置 507 や上記他の装置の処理能力が比較的低い場合であっても、保護ドキュメント 13 の生成などの処理を適切に行うことができる。

【0181】

図 16（A）及び図 16（B）に示す電子ファイル管理装置 507 の他の例を図 17 で

説明する。図17は、本発明の第4の実施形態に係る電子ファイル管理装置の他の例を示す図である。図17(A)及び図17(B)に示す電子ファイル管理装置507-2において、オリジナルのドキュメント11-2のみを管理するようにすることもできる。

【0182】

図17(A)において、ドキュメント管理プログラム71がドキュメント11-2のみを受け取って保存する際、ドキュメント管理プログラム71は、受け取ったドキュメント11-2を、直接ドキュメント管理DB23に格納する。また、図14(B)において、ドキュメント管理プログラム71は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント11-2に対するアクセス要求に対してドキュメント11-2を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ACL12との比較によるユーザのread権限の判断は行わない。

【0183】

次に、第4の実施形態に係るドキュメント管理プログラム71によって実現される機能構成について図18で説明する。図18は、第4の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアントc1-2及びc2は、同一クライアントであってもよい。

【0184】

図18において、ドキュメント管理プログラム71によって、少なくとも、ドキュメント保管要求受付部71aと、ドキュメント保管部71bと、ドキュメント参照要求受付部71dと、ドキュメント取得部71eとが機能として構成される。

【0185】

また、ドキュメント管理プログラム71の外部で保護ドキュメント13を作成してから保管する仕組みの場合、ドキュメント保管要求を行うクライアントc1-2は、ドキュメント保管要求部71fと、保護ドキュメント取得部71gとを有する。

【0186】

ドキュメント保管要求部71fは、保護ドキュメント取得部71gにドキュメント11とACL12とを渡す。保護ドキュメント取得部71gは受け取ったドキュメント11とACL12をドキュメント保護プログラム511に渡して保護ドキュメント13を取得し、その保護ドキュメント13をドキュメント保管要求部71fに返す。

【0187】

ドキュメント保管要求部71fは、ドキュメント保管要求を行うクライアントc1-2として、ドキュメント管理プログラム71にドキュメント保管要求とともにドキュメント11と、保護ドキュメント13と、ACL12とを渡す。

【0188】

ドキュメント管理プログラム71のドキュメント保管要求受付部71aは、ドキュメント保管要求を行ったクライアントc1-2からドキュメント保管要求とともにドキュメント11と、保護ドキュメント13と、ACL12とを受け取ると、それらをドキュメント保管部71bに渡す。

【0189】

ドキュメント保管部71bは、受け取ったドキュメント11と保護ドキュメントとをドキュメント・ペアとしてドキュメント管理DB23に格納し、そのドキュメント・ペアに受け取ったACL12を付与する。ドキュメント・ペアの識別子をドキュメントIDとしてドキュメント保管要求受付部71aに返す。

【0190】

ドキュメント保管要求受付部71aは、ドキュメントIDをドキュメント保管要求をしたクライアントc1-2に返す。

【0191】

ドキュメント管理プログラム71において、ドキュメント参照要求を行うクライアントc2からドキュメント参照要求を受け取ったときの流れは図4と同様であるので、説明を省略する。

【0 1 9 2】

次に、上述した各実施形態で、印刷用端末 5 0 3 に接続されたプリンタ 5 0 2 から機密印刷にて出力させる場合について説明する。

【0 1 9 3】

先ず、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を図 1 9 で説明する。図 1 9 は、プリンタが備えるセキュリティ機能の例を示す図である。

【0 1 9 4】

図 1 9 において、まず、印刷要件として P A C が設定されている場合のドキュメント印刷プログラム 5 2 1 の動作について説明する。P A C が設定されている場合のドキュメント印刷プログラム 5 2 1 の動作を図 2 0 に示す。

【0 1 9 5】

(1) ドキュメント印刷プログラム 5 2 1 は P A C が設定されているドキュメントファイルを印刷する際には、図 2 1 に示すように、プリントダイアログ 5 5 8 を表示させた後に個人識別番号 (Personal Identification Number: P I N) を入力する P I N 入力ダイアログ 5 5 9 を印刷用端末 5 0 3 の表示装置に表示させ、ユーザに P I N の入力を要求する。

【0 1 9 6】

(2) 印刷用端末 5 0 2 の入力装置を用いてユーザが P I N を入力すると、ドキュメント印刷プログラム 5 2 1 は、これをプリンタドライバ 5 0 3 b に設定し、印刷を指示する。

【0 1 9 7】

プリンタドライバ 5 0 3 b は、ドキュメントから Postscript P D L (Page Description Language) で記述された印刷データ (P D L データ) を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述した P J L (Print Job Language) データを P D L データの先頭に付加する。プリンタドライバ 5 0 3 b はさらに P J L データの一部として P I N を付加し、その P J L データ付き P D L データをプリントエンジン 5 0 3 a に送る。

【0 1 9 8】

プリンタ 5 0 3 は、P J L データ付き P D L データを受け取ると P J L データの内容を参照し、機密印刷用の P I N が含まれている場合は印刷出力せずにプリンタ 5 0 3 内部の記憶装置 (HDD など) に P J L データ付き P D L データを保存する。ユーザが P I N をプリンタ 5 0 3 のオペレーションパネルを介して入力すると、プリンタ 5 0 3 は入力された P I N を P J L データに含まれる P I N と照合し、一致すれば P J L データに含まれていた印刷ジョブ条件 (部数、トレイなど) を適用しながら P D L データに従って印刷出力する。

【0 1 9 9】

(3) プリンタドライバ 5 0 3 b に P I N が設定できない、すなわち、プリンタ 3 が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。

【0 2 0 0】

このようにすることで、印刷実行後、プリンタ 5 0 3 のオペレーションパネルにおいて印刷実行前に入力したものと同一の P I N が入力されるまでドキュメントのプリントアウトがプリンタ 5 0 3 から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ 5 0 3 に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。

【0 2 0 1】

さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ 5 0 3 とやりとりを S S L で保護してもよい。

【0 2 0 2】

また、ドキュメント印刷プログラム 5 2 1 を Windows (登録商標) Domain のユーザ管理

と連動させて、ユーザに対して P I N の入力进行を要求しないようにしてもよい。例えば、P I N をユーザに入力させるのではなく、Windows (登録商標) Domain から現在ログオン中のユーザ I D を取得し、プリントデータとともにユーザ I D をプリンタ 5 0 3 へ送付するようにする。プリンタ 5 0 3 は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザ I D とパスワードとで Windows (登録商標) Domain のユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows (登録商標) Domain に限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒な P I N 入力の手間を削減できる。

【0203】

次に、印刷要件として E B C が設定されている場合のドキュメント印刷プログラム 5 2 1 の動作について説明する。

【0204】

(1) ドキュメント印刷プログラム 5 2 1 は、E B C が設定されているドキュメントを印刷する際にドキュメント I D を示すバーコード画像データ (又は、二次元コード) のデータを生成する。

【0205】

(2) ドキュメント印刷プログラム 5 2 1 は、生成したバーコード画像データをスタンプ画像としてプリンタドライバ 5 0 3 b にセットし、プリンタ 5 0 3 に印刷を指示する。

【0206】

(3) プリンタドライバ 5 0 3 b に E B C が設定できない、すなわち、プリンタ 5 0 3 がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0207】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメント I D を取得し、そのドキュメント I D を基にアクセスコントロールサーバ 5 0 4 が、ハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【0208】

次に、印刷要件として B D P が設定されている場合のドキュメント印刷プログラム 5 2 1 の動作について説明する。

【0209】

(1) ドキュメント印刷プログラム 5 2 1 は、B D P が設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する (例えば、Ichiro, 2002/08/04 23:47:10)。

【0210】

(2) ドキュメント印刷プログラム 5 2 1 は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

【0211】

(3) ドキュメント印刷プログラム 5 2 1 は、生成した地紋画像をスタンプとしてプリンタドライバ 5 0 3 b にセットし、プリンタ 5 0 3 にドキュメントの印刷を指示する。

【0212】

(4) プリンタドライバ 5 0 3 b に B D P が設定できない場合、すなわちプリンタ 5 0 3 が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0213】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、E B C をサポートし

ていない複写機をしようとする場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【0 2 1 4】

次に、印刷要件として S L S が設定されている場合のドキュメント印刷プログラム 5 2 1 の動作について説明する。

【0 2 1 5】

(1) ドキュメント印刷プログラム 5 2 1 は、S L S が設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの (Top Secret ならば「極秘」のマークなど) を選択する。

【0 2 1 6】

(2) 選択した画像のデータを、スタンプとしてプリンタドライバ 5 0 3 b にセットし、プリンタ 5 0 3 に印刷を指示する。

【0 2 1 7】

(3) プリンタドライバ 5 0 3 b に S L S をセットできない場合、すなわち、プリンタ 5 0 3 が S L S をサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【0 2 1 8】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【0 2 1 9】

上記の各例は、あくまでも印刷要件の一例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する (印刷に使用する用紙トレイを特殊用紙のトレイに限定する) ようにしてもよい。

【0 2 2 0】

このように、プリンタ 5 0 3 がサポートする様々なセキュリティ機能を利用してセキュリティポリシーを設定することによって、プリンタ 5 0 3 のセキュリティ機能が無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは上述した各実施形態のシステム構成においても同様である。

【0 2 2 1】

上記各実施例において共通のユーザにて提供される画面について図 2 2 から図 2 6 で説明する。

【0 2 2 2】

図 2 2 は、電子ファイル管理装置にアクセスした際に表示される画面例を示す図である。図 2 2 において、例えば、管理者としてのユーザが、ユーザが利用しているクライアントの画面 5 5 0 に表示される文書管理 5 5 1 を選択すると、ユーザを認証するためのダイアログ 5 5 2 が表示される。画面 5 5 2 のユーザ名及びパスワードの入力域 5 5 3 に、ユーザがユーザ名及びパスワードを入力し、認証を実行するために OK ボタン 5 5 4 をクリックすると、電子ファイル管理装置 5 1 1 にてユーザの認証が行われる。一方、ユーザがキャンセルボタン 5 5 5 をクリックすると、電子ファイル管理装置 5 1 1 へのアクセスがキャンセルされる。

【0 2 2 3】

ユーザの認証に成功すると、次のように電子ファイル管理装置 5 0 1 にて管理されているドキュメントの一覧を、例えば、図 2 3 に示すように表示する。図 2 3 は、電子ファイル管理装置にて管理されるドキュメントの一覧を表示する画面例を示す図である。

【0 2 2 4】

図 2 3 において、画面 5 6 0 は、ユーザの認証が成功した場合に表示される場面であって、電子ファイル管理装置 5 0 1 にて管理されるドキュメントの一覧を表示する。

【0 2 2 5】

ドキュメントの一覧として、フォルダ1、フォルダ2、フォルダ3、及びフォルダ4、文書01、文書02、及び文書03とが表示される。フォルダ1から4は、例えば、フォルダの形状を示すアイコンで表示され、文書01から03は、例えば、サムネイルで表示される。

【0226】

例えば、ユーザが文書02を選択すると、ドキュメント参照要求が電子ファイル管理装置501に送信され、文書02に対するアクセス権が確認される。参照権限がある場合には、文書02の保護ドキュメントだけをクライアントに提示する。

【0227】

図24は、保護ドキュメントが提示されている画面例を示す図である。図24において、画面570では、文書02として文書02の保護ドキュメントが提供されることがアイコン571によって示される。例えば、アイコン571は、PDFファイルを示しており、有効の状態が表示されることによって、文書02の保護ドキュメントしかアクセスできないことを示す。

【0228】

文書02を示すサムネイル572では、例えば、左端にオリジナルのドキュメントがMS Word（登録商標）のファイル形式を示すアイコン573が表示される。

【0229】

クライアント側では文書02の保護ドキュメントを開くために、ダイアログ574を表示して、再度ユーザ認証が求められる、先のユーザ認証で入力されたものを自動的に使用するようにしても良い。

【0230】

ダイアログ574に設定された認証情報による認証が生協すると、例えば、図25に示されるような画面が表示される。図25は、保護ドキュメントが開かれた状態を示す図である。

【0231】

図25において、画面580は、文書02の保護ドキュメントに対するユーザ認証が成功し、かつ、保護ドキュメントを開く権限があった場合に、開かれた保護ドキュメントを表示する。

【0232】

そして、ユーザは、文書02の保護ドキュメントの内容を参照することができ、更に、印刷権限があればこの保護ドキュメントを印刷することができる。つまり、ユーザが印刷するためのアイコン581をクリックすると、印刷権限がこのユーザにあるか否かが確認され、規定されているこの文書02に対するセキュリティの要件を満たすように処理が行われ印刷される。

【0233】

一方、図24に示す画面570において、ユーザがオリジナルの文書02を参照する場合について図26で説明する。図26は、ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図である。

【0234】

図26において、ユーザがアイコン575をクリックすることによって、オリジナルの文書02にアクセスしようとする、ユーザにオリジナルの文書02にアクセスする権限があるか否かが判断される。ユーザにオリジナルの文書02を参照する権限がない場合には、「セキュリティポリシーによるオリジナル参照権限が与えられていません。」等のメッセージを示すダイアログ576が表示される。従って、ユーザは、オリジナルの文書02を参照することができない。

【0235】

なお、上述した各実施形態は、本発明の好適な実施形態であり、本発明の主旨を逸脱しない範囲内において、種々変形して実施することが可能である。

【0236】

例えば、上述した各実施形態で用いられる各種ドキュメント（電子ファイル）の内容は、文書に限定されず、例えば画像を含めた文書ファイルや画像ファイルなどであってもよい。

【0237】

また、本発明に係る電子ファイル管理装置が入力装置と表示装置とを備えることとしているが、この構成に限定されず、例えば、ネットワークを介して接続されたユーザ端末により電子ファイル管理装置がユーザからの入力を受けたり、ネットワークを介して接続された表示装置や外部記録装置に電子ファイル管理装置から出力したりしてもよい。

【0238】

また、プリンタを電子ファイル管理装置や印刷用端末に接続して出力に用いる場合、ネットワークを介して接続されたものであっても、電子ファイル管理装置や印刷用端末と一体化されたものであってもよい。

【0239】

また、格納装置が複数ある場合、ACLなどが付与されていることを確認できるのであれば（例えば、上述のように関連付けて格納する、など）、ドキュメント・ペアのそれぞれやACLを異なる格納部に格納してもよい。

【0240】

また、以上に、ドキュメント保護プログラムとしてユーザベース・アクセス制御モデルのものを利用した場合の実施形態について説明したが、アクセス権限を管理するための情報を設定して電子ファイルの管理を行うことができれば本発明はこのものに限定されない。例えば、ポリシーベース・アクセス制御モデルのドキュメント保護プログラムを利用した場合には、ACLではなくポリシーに従ってアクセスが制御されるだけで基本的には同じ仕組みとして本発明は同様に適用可能である。

【図面の簡単な説明】

【0241】

【図1】 本発明の第1の実施形態に係る電子ファイル管理装置を示す図である。

【図2】 ACLの構成例を示す図である。

【図3】 ドキュメント保護・印刷システムの構成を示す図である。

【図4】 第1の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図5】 ドキュメント保護プログラムの動作を示す図である。

【図6】 ACLデータベースに記録される情報の構造例を示す図である。

【図7】 ドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図8】 アクセスコントロールへのSOAPによる問い合わせの例を示す図である。

【図9】 本発明の第1の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図10】 本発明の第2の実施形態に係る電子ファイル管理装置を示す図である。

【図11】 本発明の第2の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図12】 第2の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図13】 第3の実施形態の電子ファイル管理装置の例を示す図である。

【図14】 本発明の第3の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図15】 第3の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図16】 本発明の第4の実施形態に係る電子ファイル管理装置を示す図である。

【図17】 本発明の第4の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図 18】 第 4 の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図 19】 プリンタが備えるセキュリティ機能の例を示す図である。

【図 20】 PAC が設定されたドキュメントを印刷する際の処理を示す図である。

【図 21】 PIN 入力のダイアログを示す図である。

【図 22】 電子ファイル管理装置にアクセスした際に表示される画面例を示す図である。

【図 23】 電子ファイル管理装置にて管理されるドキュメントの一覧を表示する画面例を示す図である。

【図 24】 保護ドキュメントが提示されている画面例を示す図である。

【図 25】 保護ドキュメントが開かれた状態を示す図である。

【図 26】 ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図である。

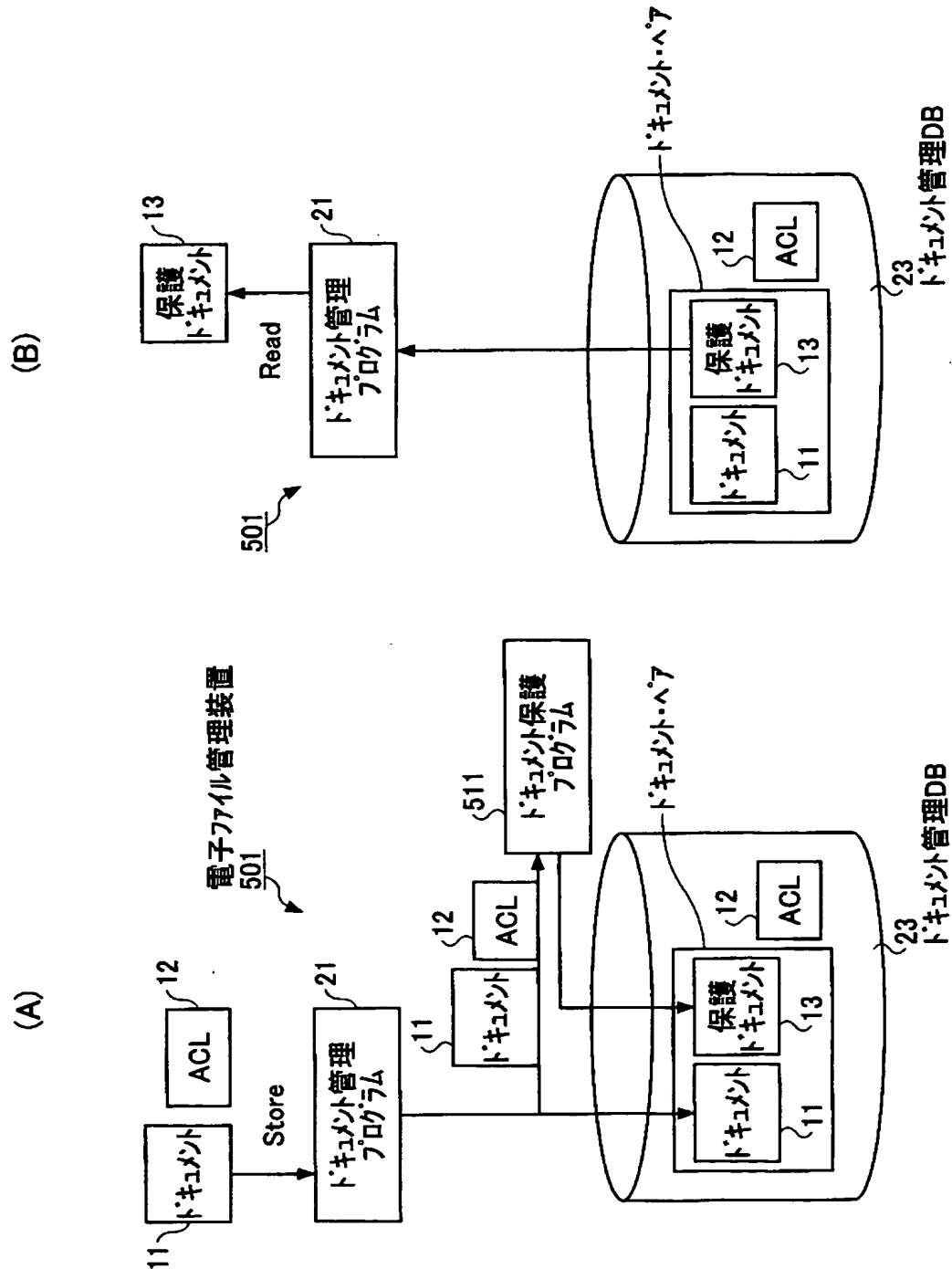
【符号の説明】

【0242】

| | |
|-----|---------------|
| 11 | ドキュメント |
| 12 | ACL |
| 13 | 保護ドキュメント |
| 21 | ドキュメント管理プログラム |
| 23 | ドキュメント管理DB |
| 501 | 電子ファイル管理装置 |
| 502 | 印刷用端末 |
| 503 | プリンタ |
| 504 | アクセスコントロールサーバ |
| 511 | ドキュメント保護プログラム |
| 521 | ドキュメント印刷プログラム |
| 541 | ユーザデータベース |
| 542 | ACLデータベース |

【書類名】 図面
【図 1】

本発明の第1の実施形態に係る電子ファイル管理装置を示す図



【図 2】

ACLの構成例を示す図

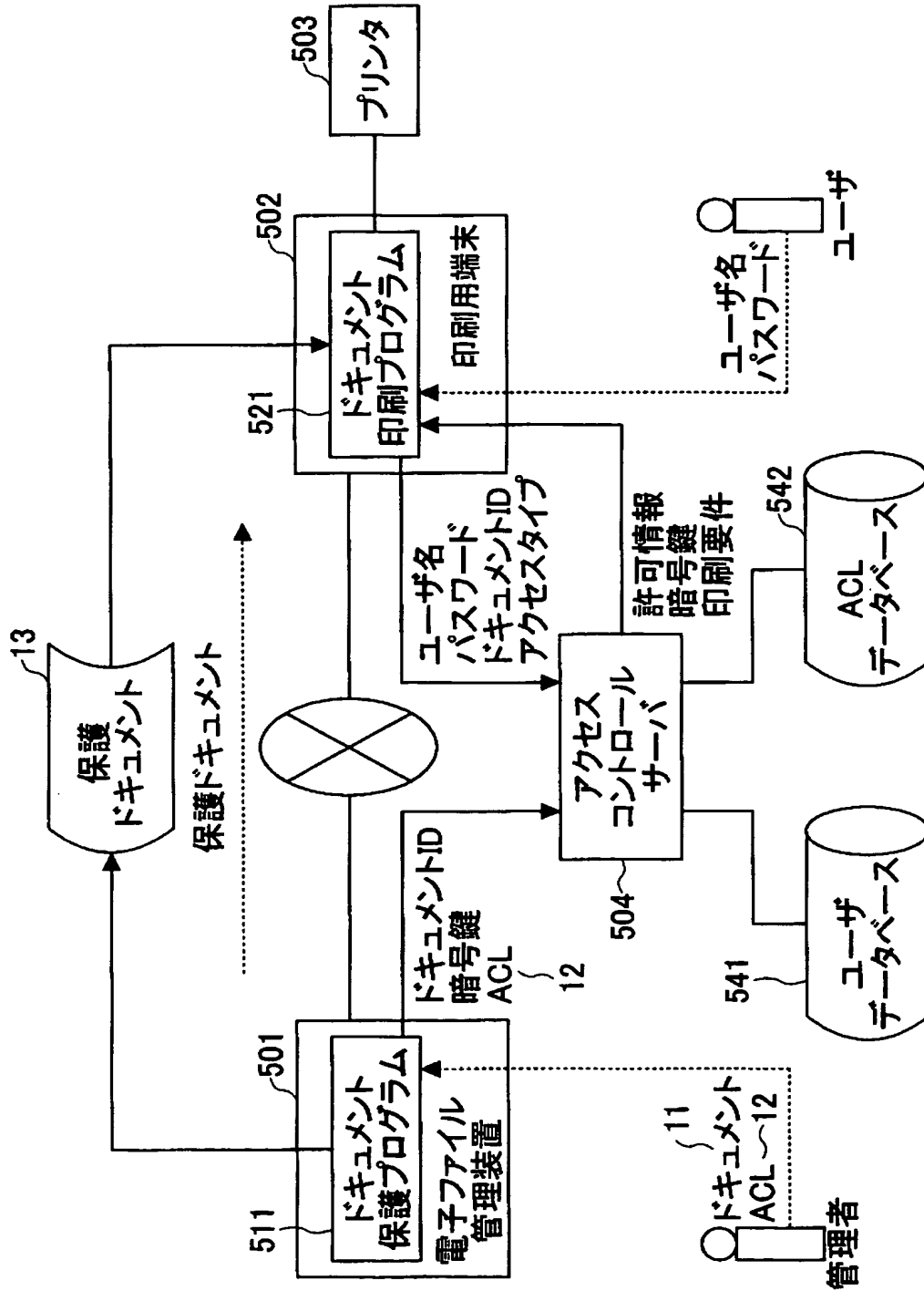
12

| User name | Access type | Permission | Requirement |
|-----------|-------------|------------|----------------------------|
| Ichiro | Read | Allowed | — |
| | Write | Denied | — |
| | Print | Allowed | PAC(Private Access) |
| | | | BDP(Background Dot Patten) |
| | | | EBC(Embedding BarCode) |
| | Hardcopy | Allowed | RAD(Record Audit Date) |
| Taro | Read | Allowed | — |
| | Write | Denied | — |
| | Print | Denied | — |
| | Hardcopy | Denied | — |
| ⋮ | | | |

【図 3】

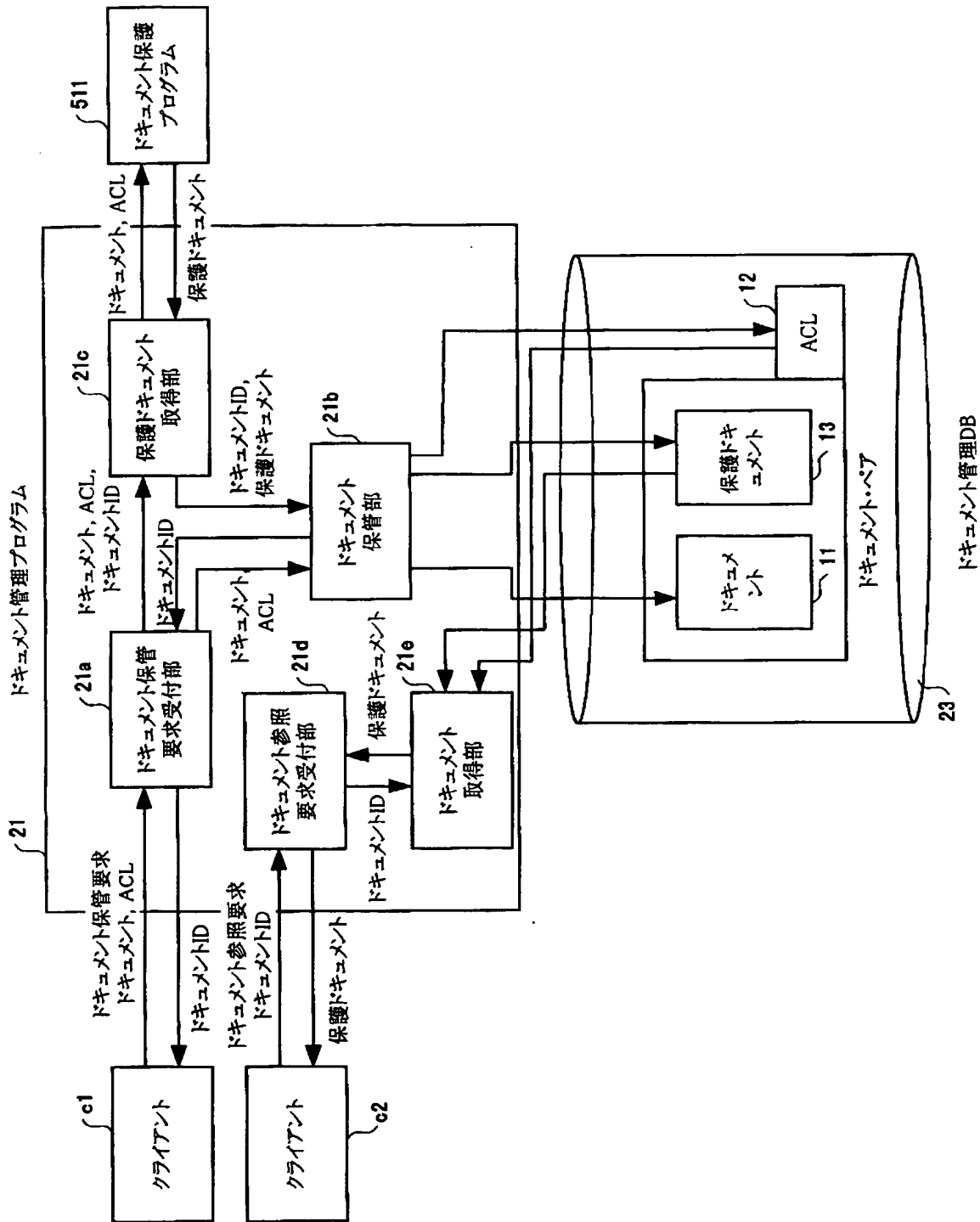
ドキュメント保護・印刷システムの構成を示す図

5001 ドキュメント保護・印刷システム



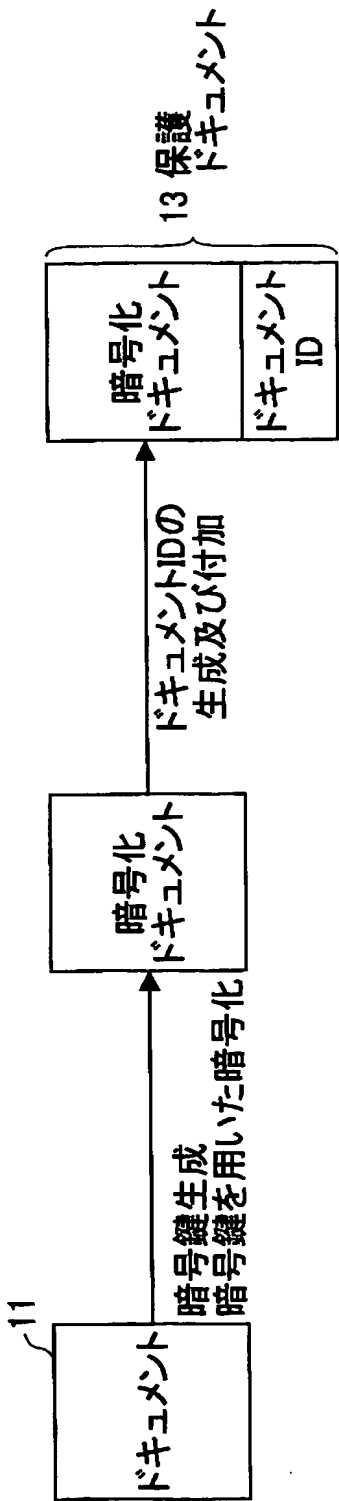
【図 4】

第1の実施形態に係るドキュメント管理プログラムによって実現される
機能構成を示す図



【図 5】

ドキュメント保護プログラムの動作を示す図



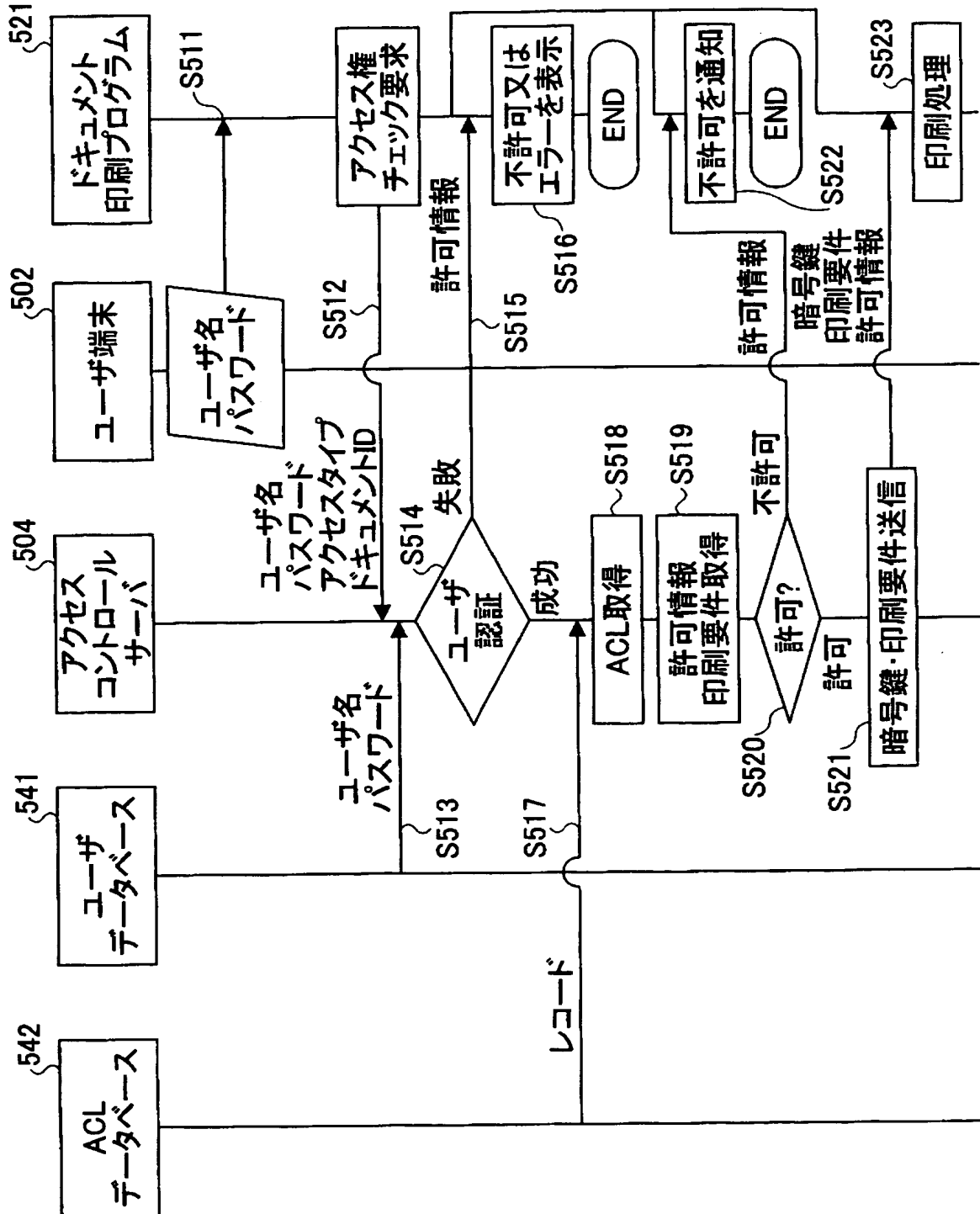
【図 6】

ACLデータベースに記録される情報の構造例を示す図

| Document ID | Key | ACL |
|------------------------------|------------|---------------|
| 133.139.234.23.22.125.98.192 | 89FECA8D2B | (binary data) |
| 133.139.234.23.22.125.99.105 | A73C44DA59 | (binary data) |
| | | |

【図 7】

ドキュメント印刷プログラム
及びアクセスコントロールサーバの動作の流れを示す図



【図 8】

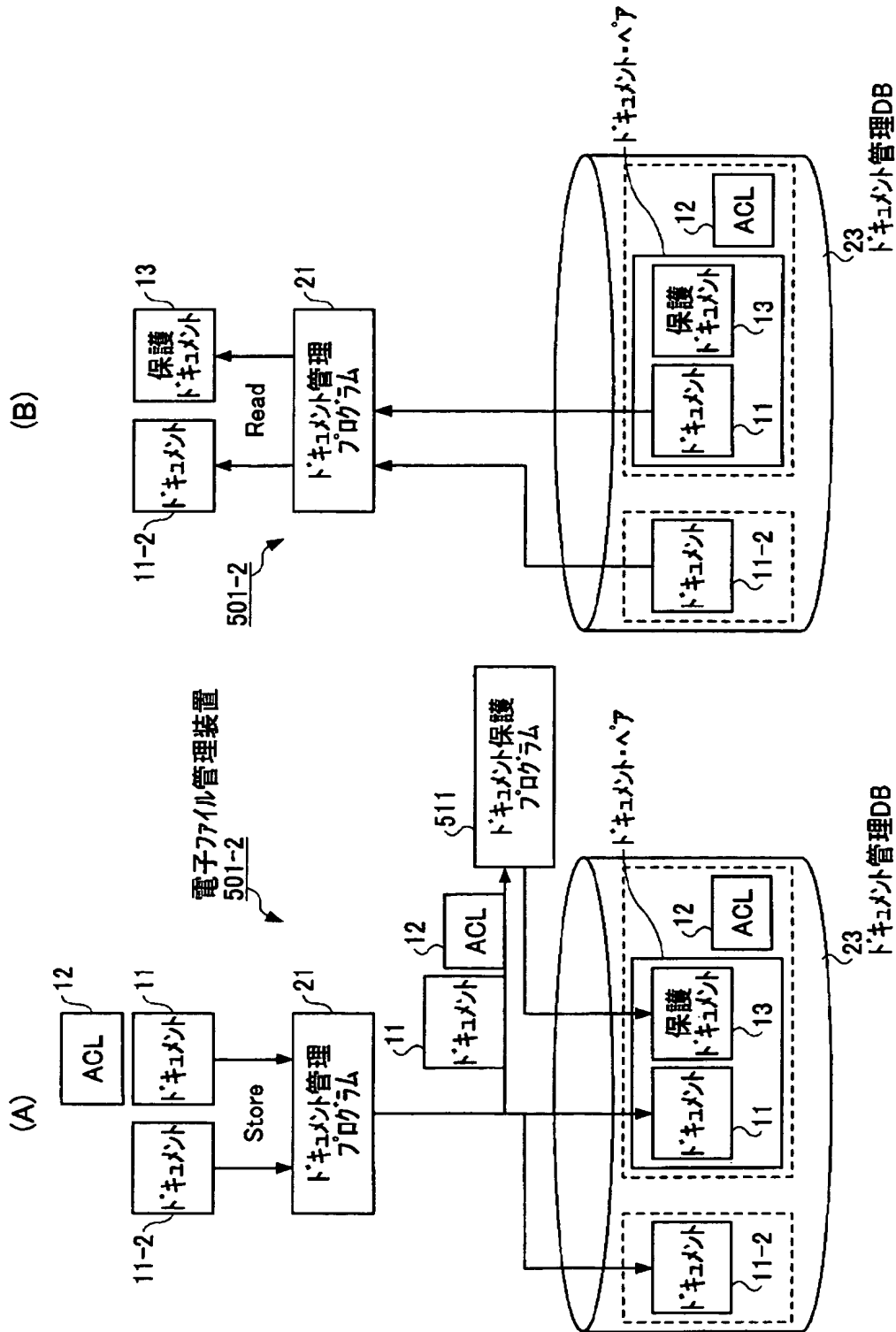
アクセスコントロールへのSOAPによる 問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowed xmlns:m="http://sample.com/sample">
      <sessionId>adfkla;iowoemads</sessionId>
      <userId>taro.yamada</userId>
      <docId>shm0000000000003</docId>
      <accessType>print</accessType>
    </m:isAllowed>
  </s:Body>
</s:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
      <isAllowedReturn>
        <allowed xsi:type="xsd:boolean">true</allowed>
        <requirements>
          <item>
            <requirement>private_access</requirement>
          </item>
          <item>
            <requirement>watermark</requirement>
          </item>
          <supplement>CONFIDENTIAL</supplement>
        </requirements>
      </isAllowedReturn>
    </m:isAllowedResponse>
  </s:Body>
</s:Envelope>
```

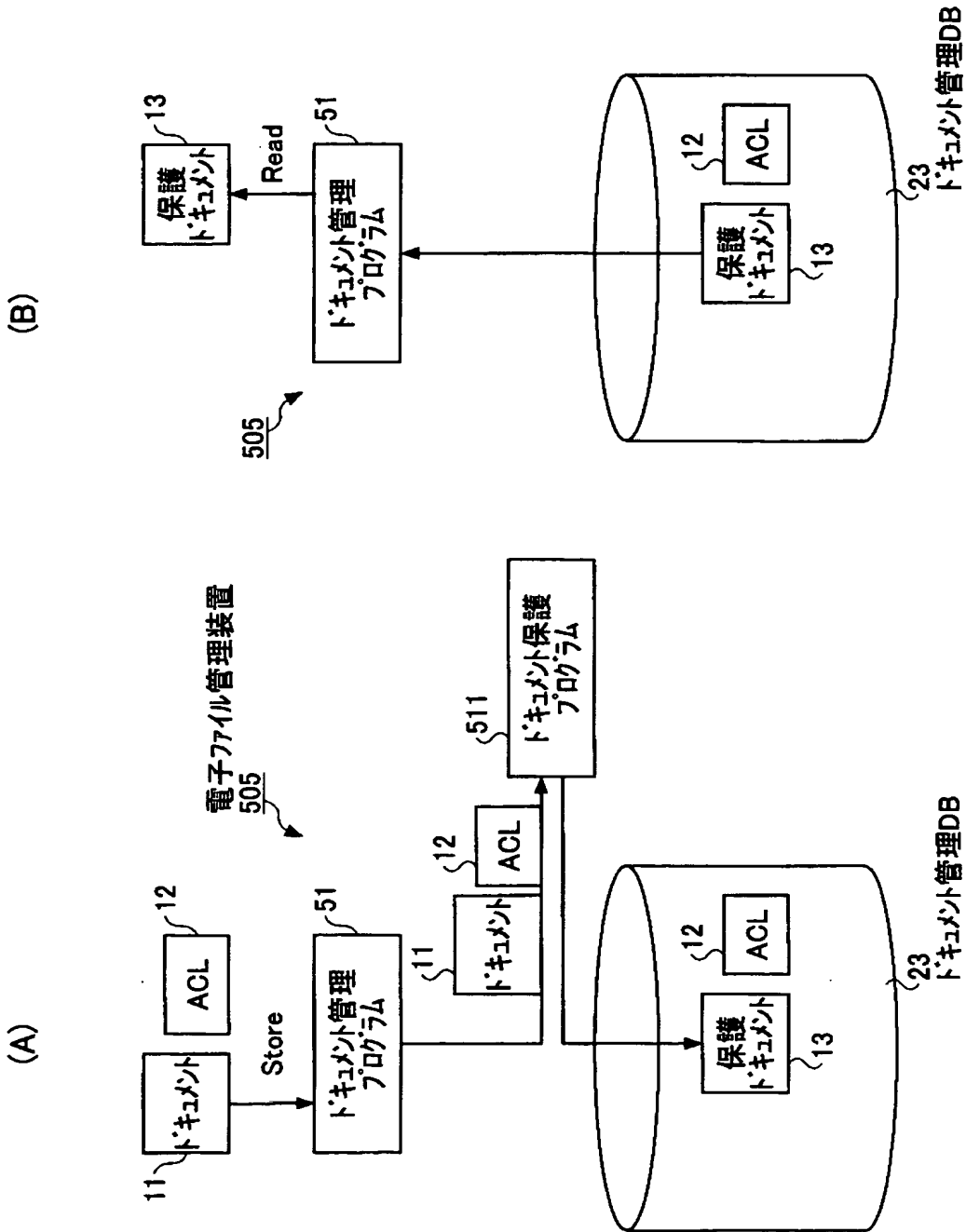
【図9】

本発明の第1の実施形態に係る電子ファイル管理装置の他の例を示す図



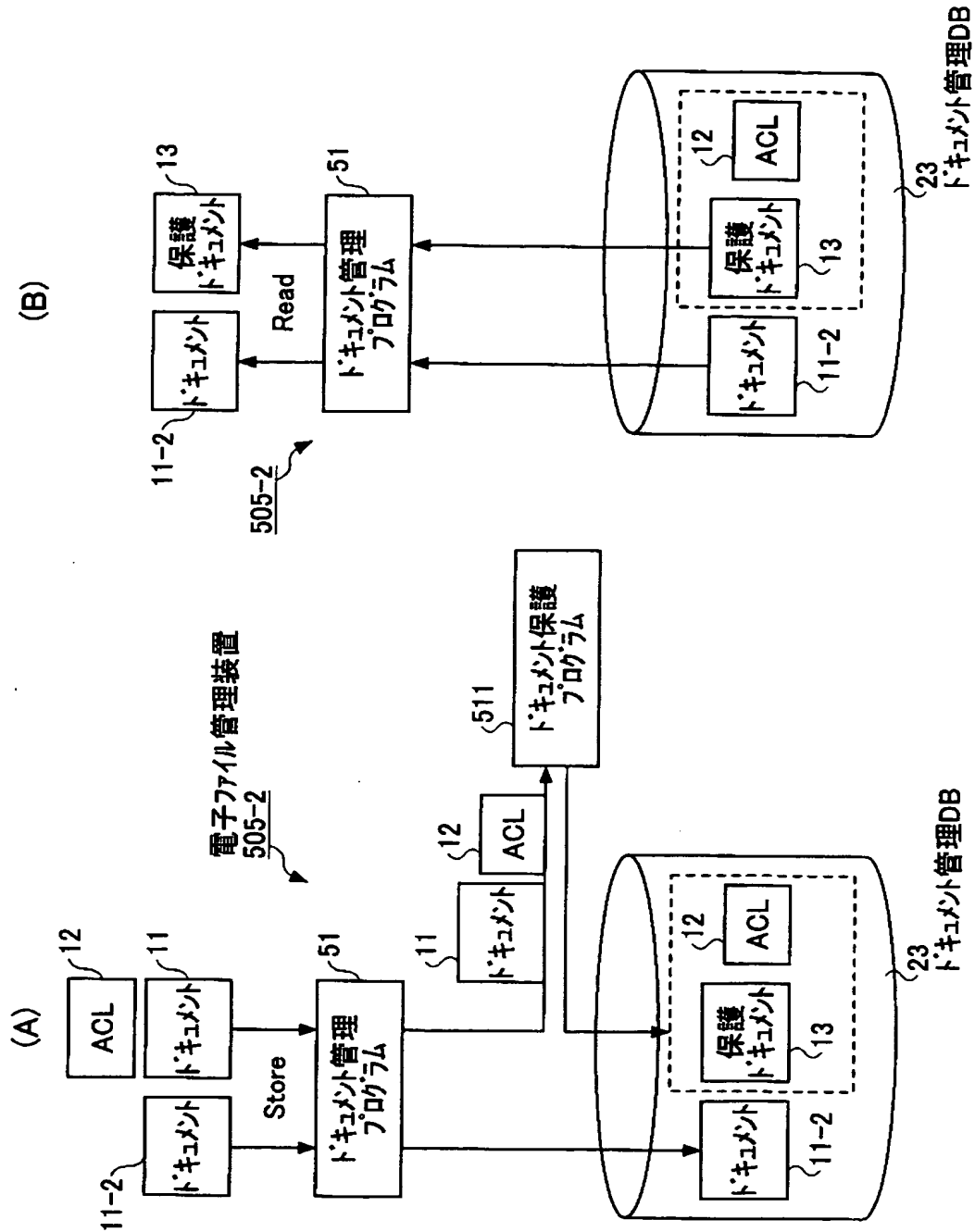
【図 10】

本発明の第2の実施形態に係る電子ファイル管理装置を示す図



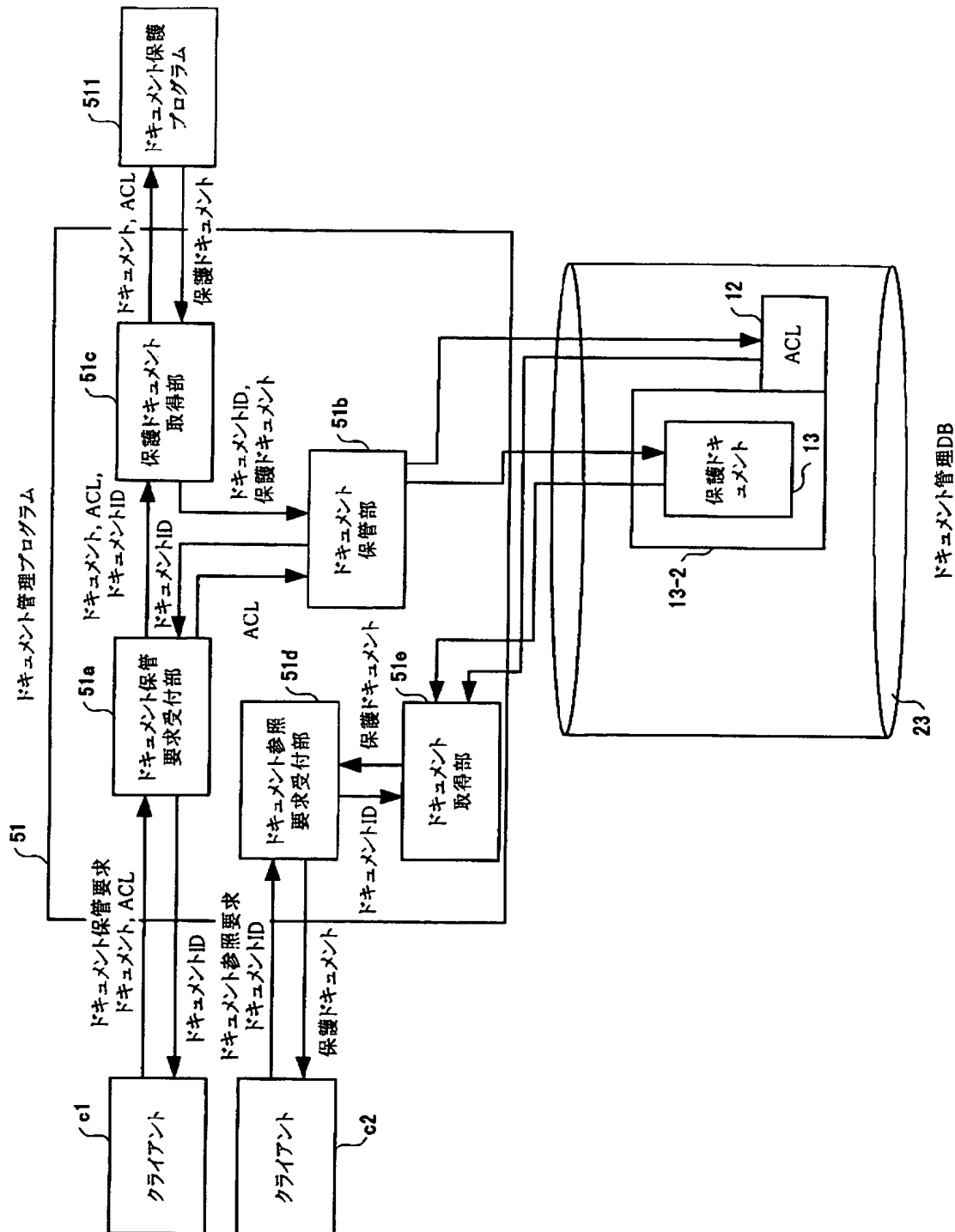
【図 11】

本発明の第2の実施形態に係る電子ファイル管理装置の他の例を示す図



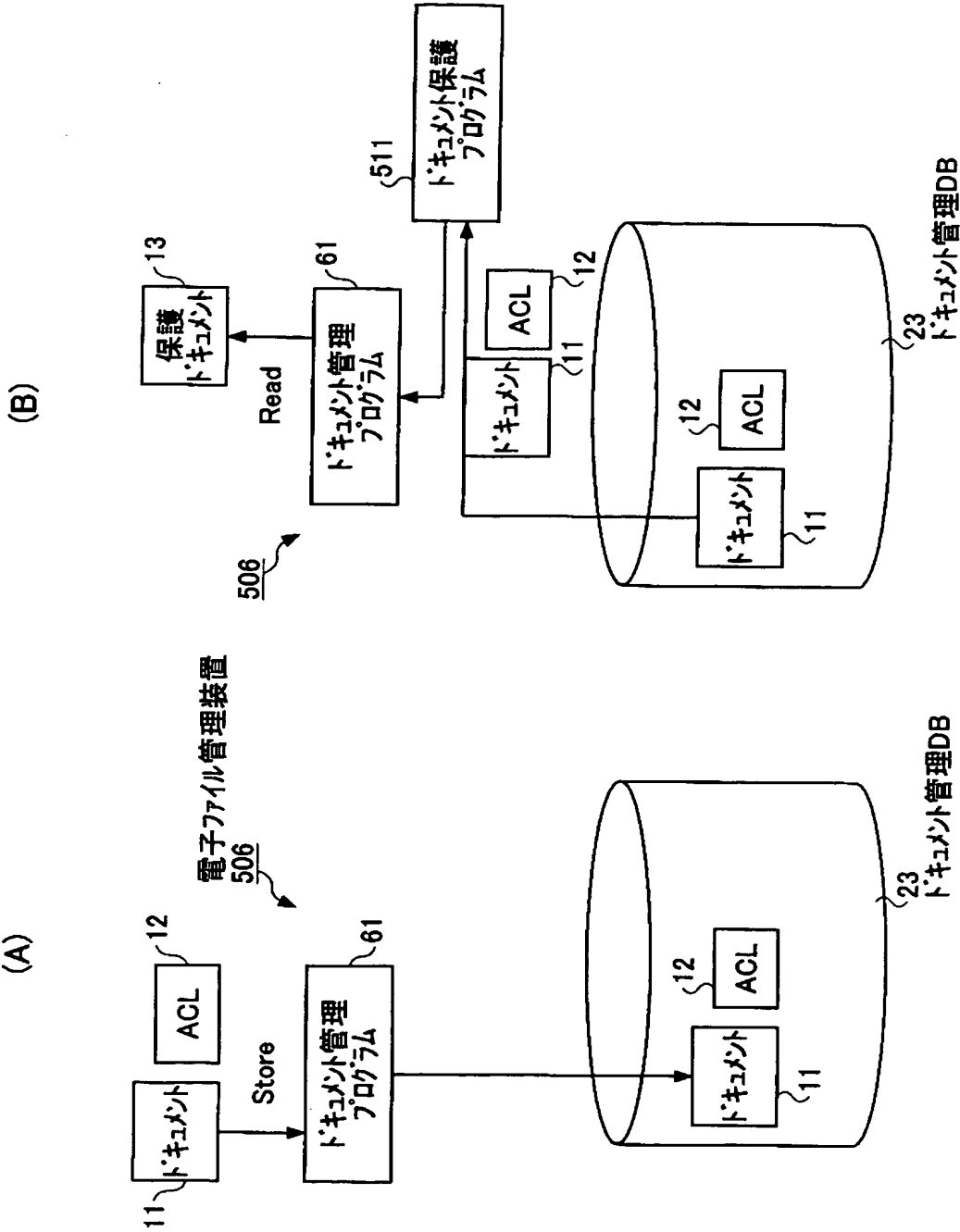
【図 12】

第2の実施形態に係るドキュメント管理プログラムによって実現される
機能構成を示す図



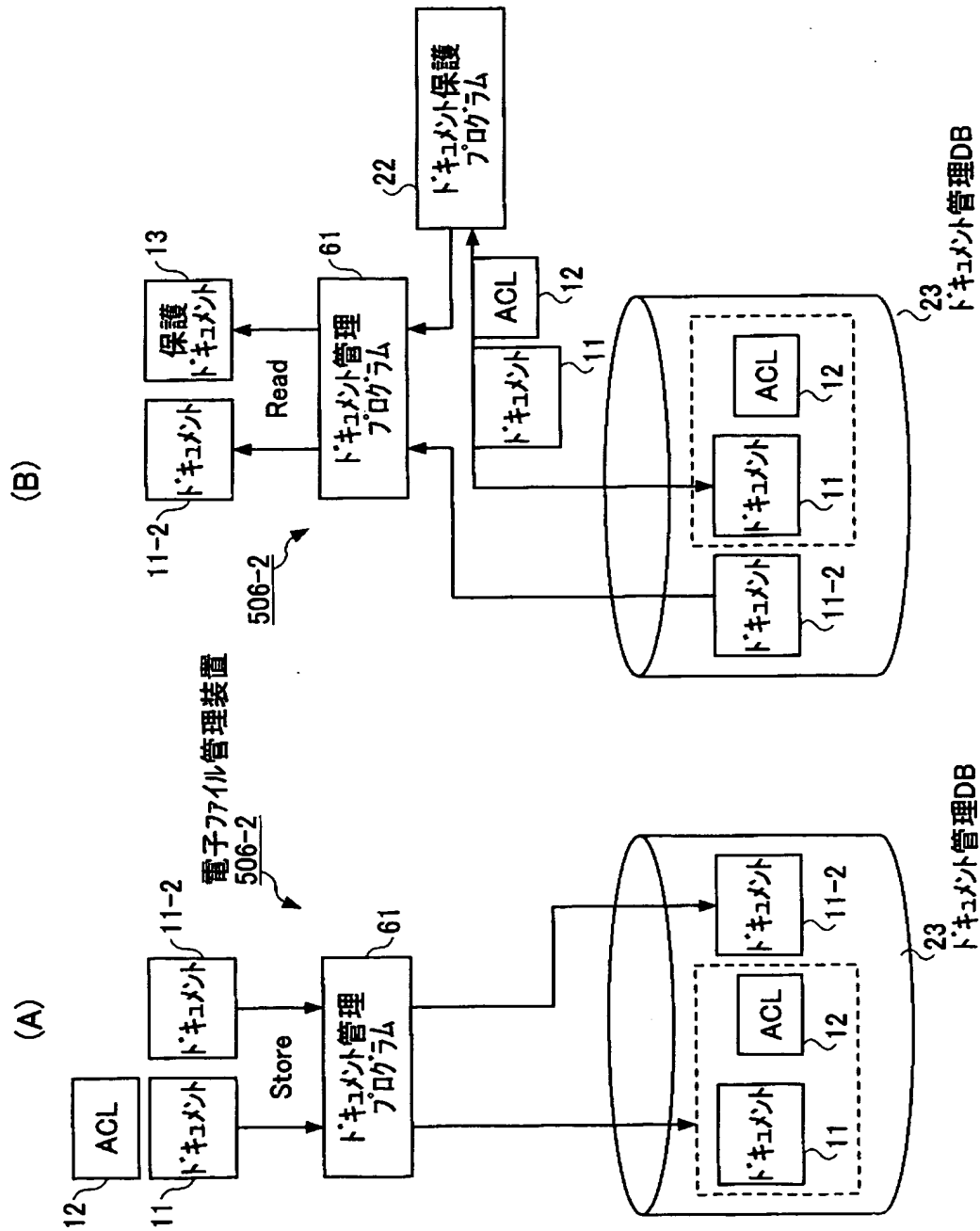
【図 13】

第3の実施形態の電子ファイル管理装置の例を示す図



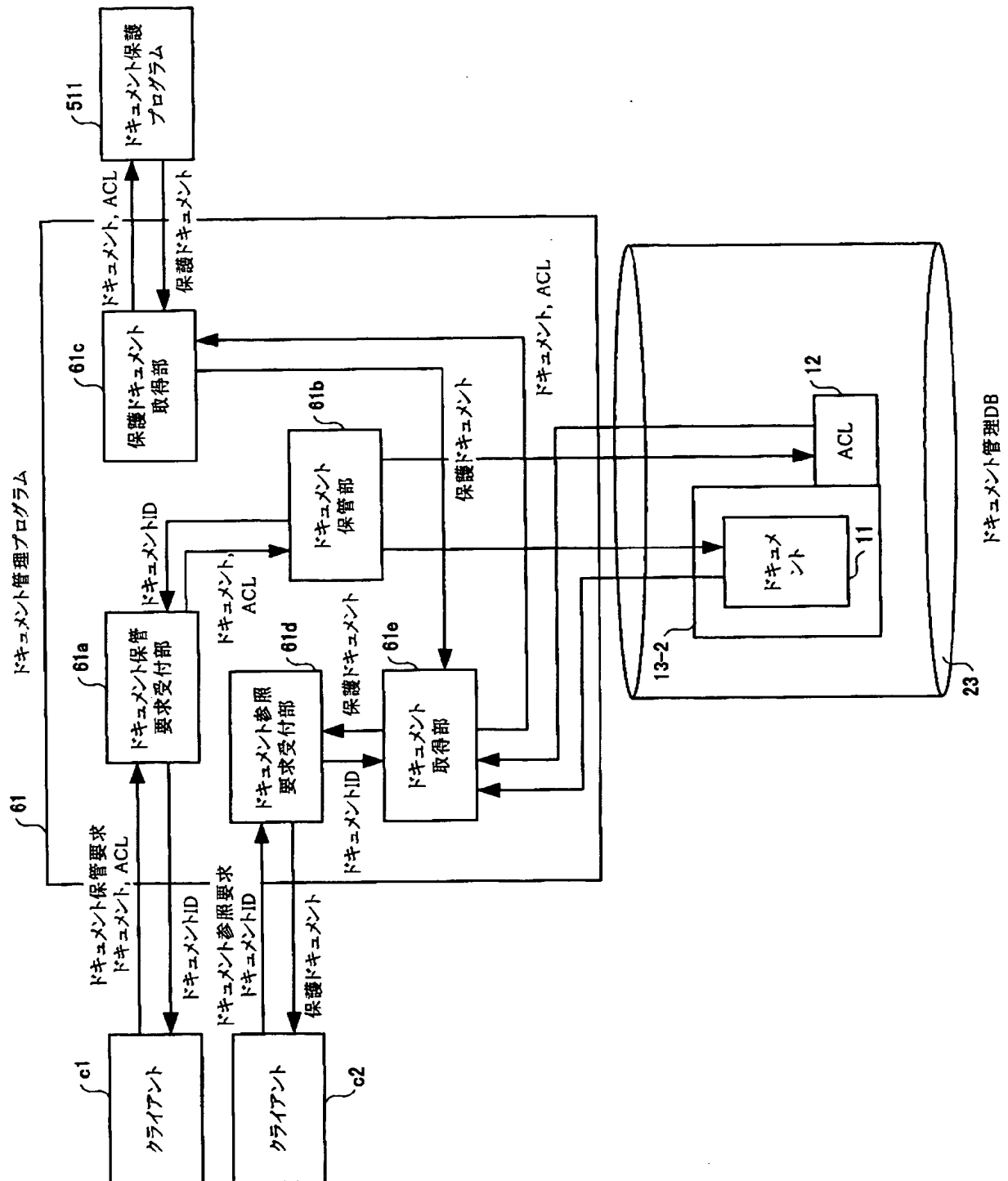
【図 14】

本発明の第3の実施形態に係る電子ファイル管理装置の他の例を示す図



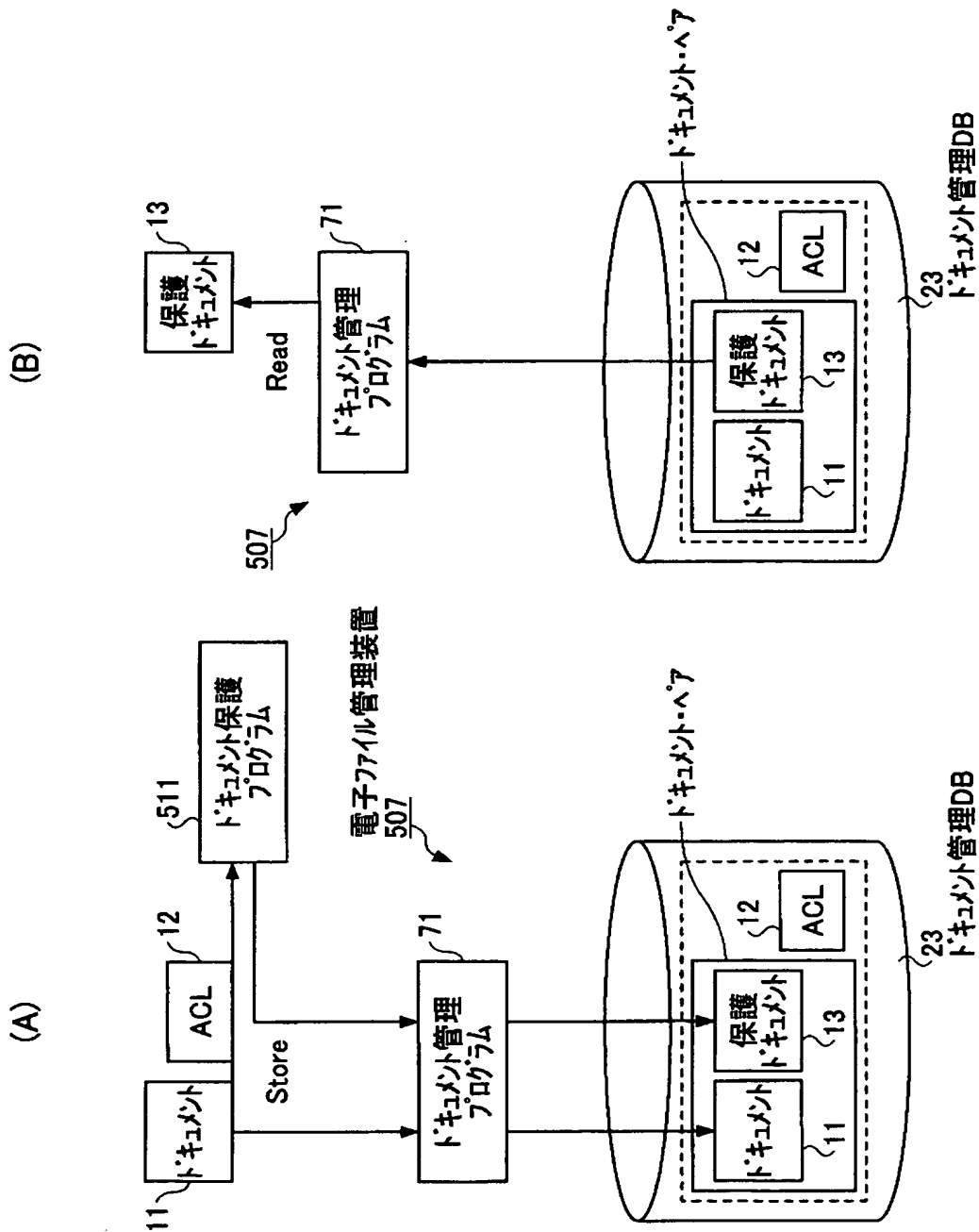
【図 15】

第3の実施形態に係るドキュメント管理プログラムによって実現される
機能構成を示す図



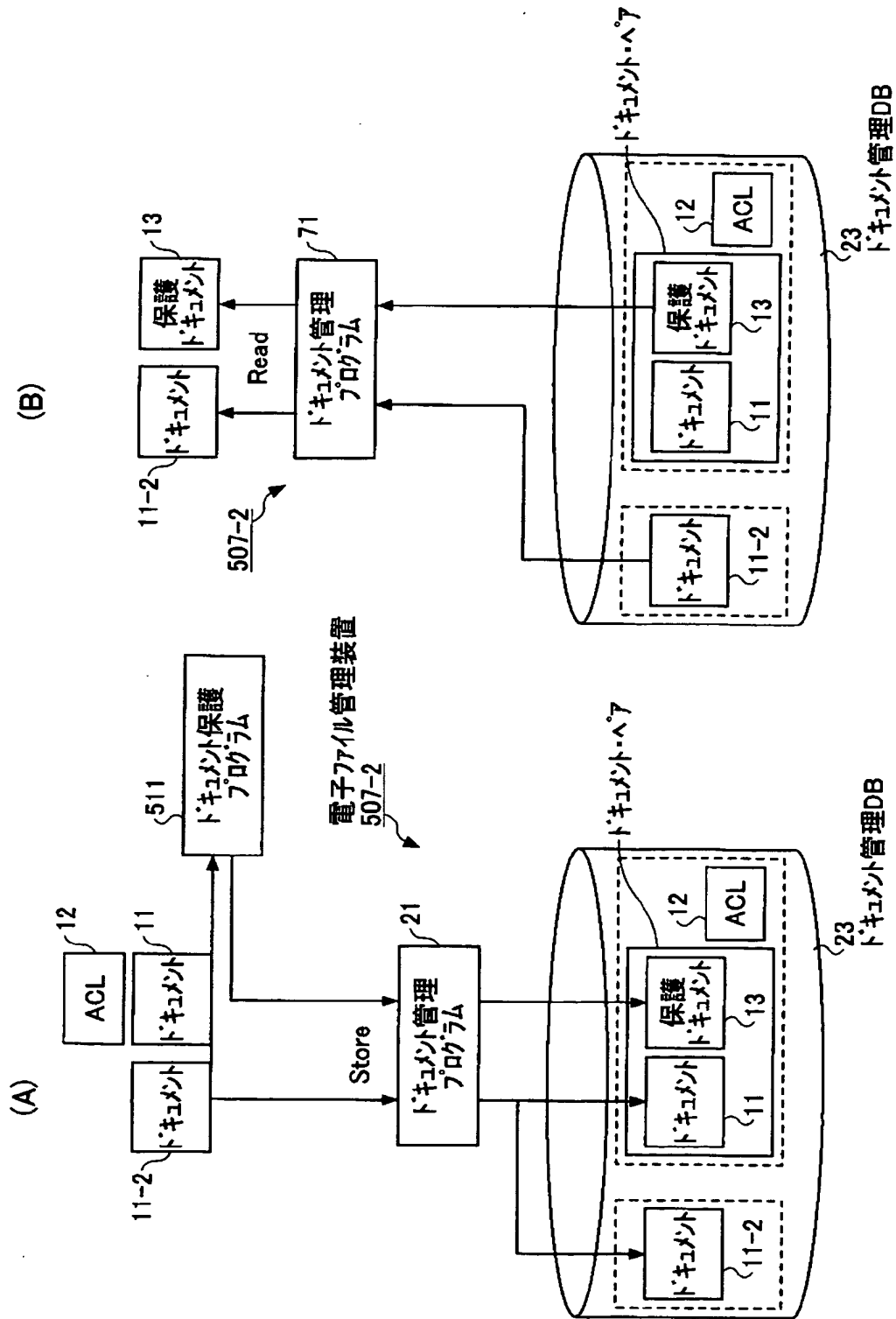
【図 16】

本発明の第4の実施形態に係る電子ファイル管理装置を示す図



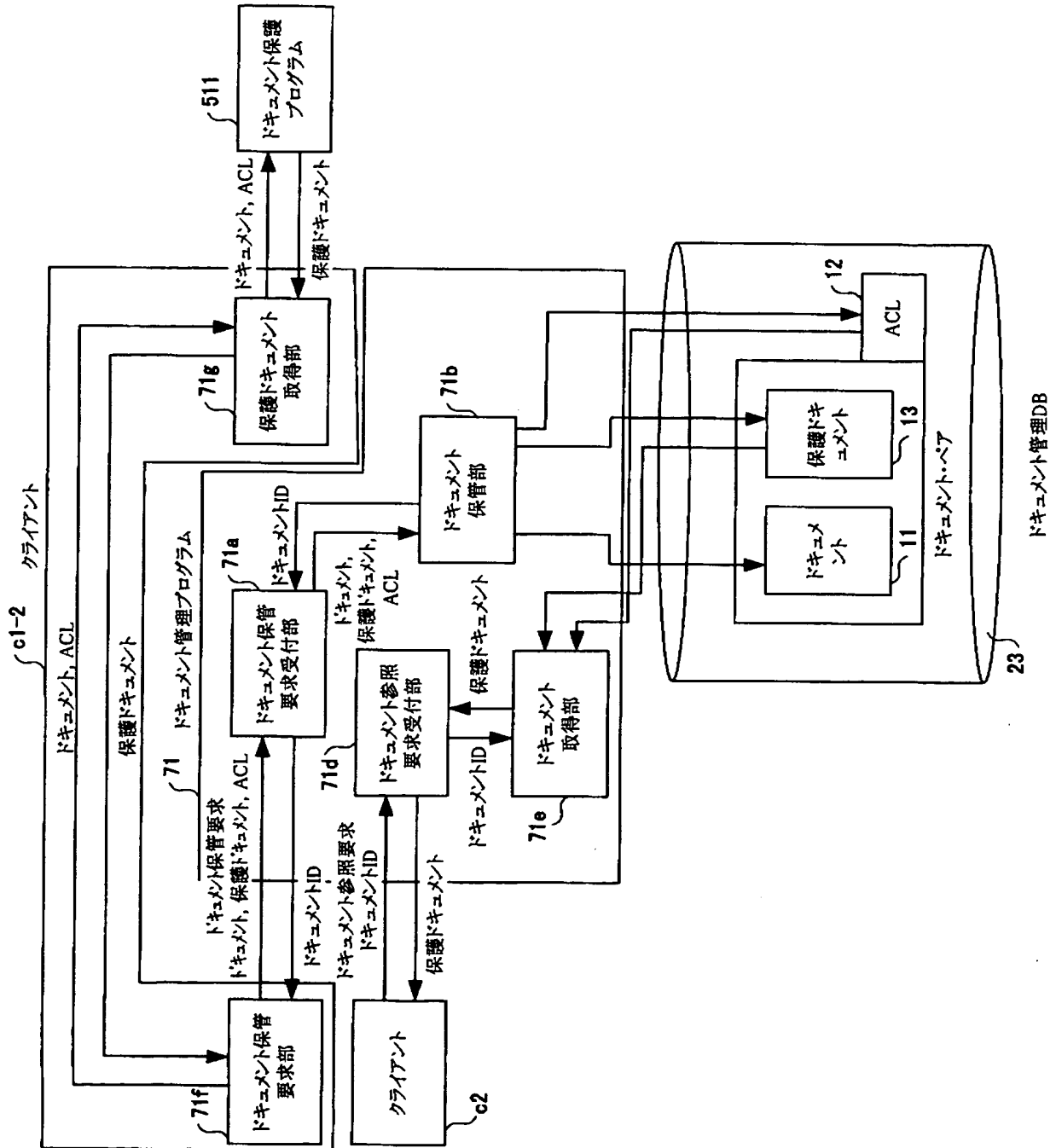
【図 17】

本発明の第4の実施形態に係る電子ファイル管理装置の他の例を示す図



【図 18】

第4の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図



【図 19】

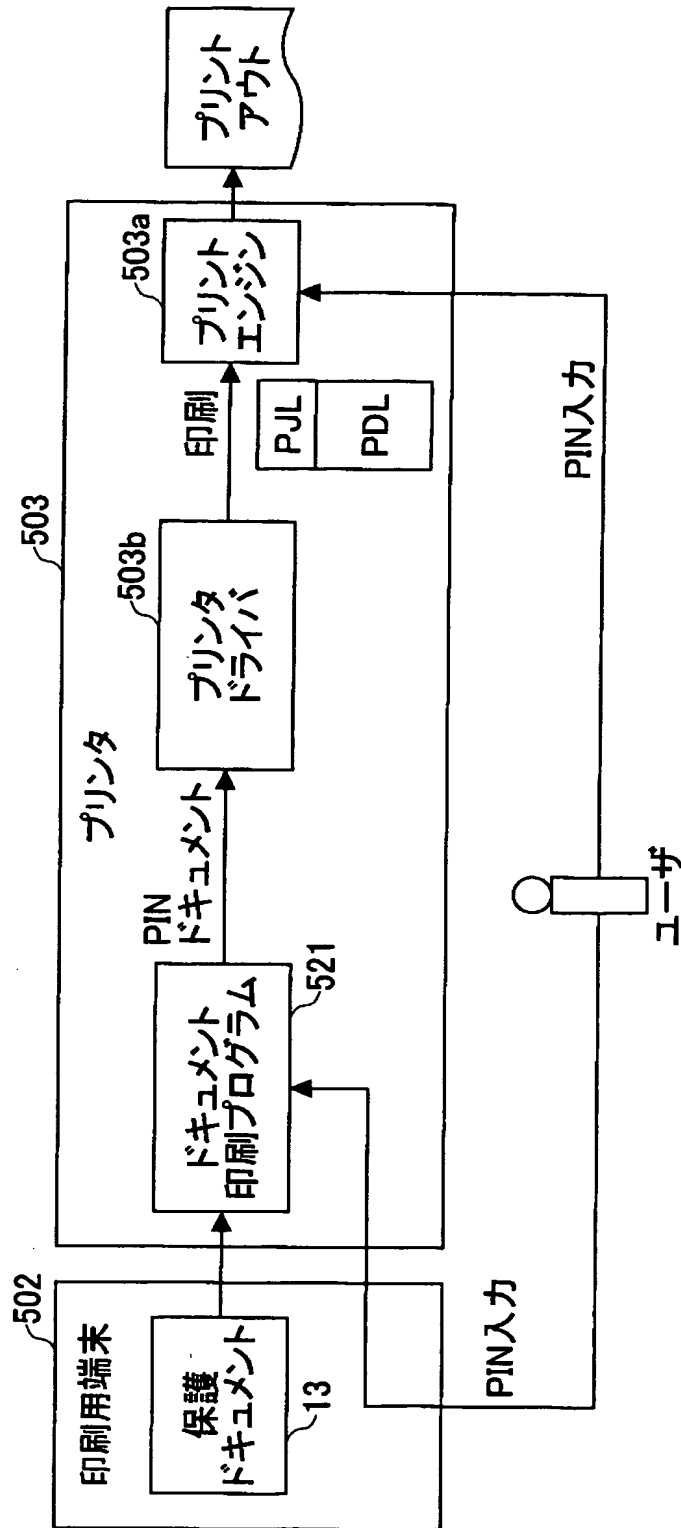
プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

| | |
|-----------------|--|
| スタンプ機能 (SLS) | マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。 |
| 地紋印刷機能 (BDP) | 複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。 |
| 機密印刷機能 (PAC) | 印刷を指示する際にプリンタドライバにPIN (Personal Identification Number) を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでそのPINを入力しなければプリントアウトされない機能。 |

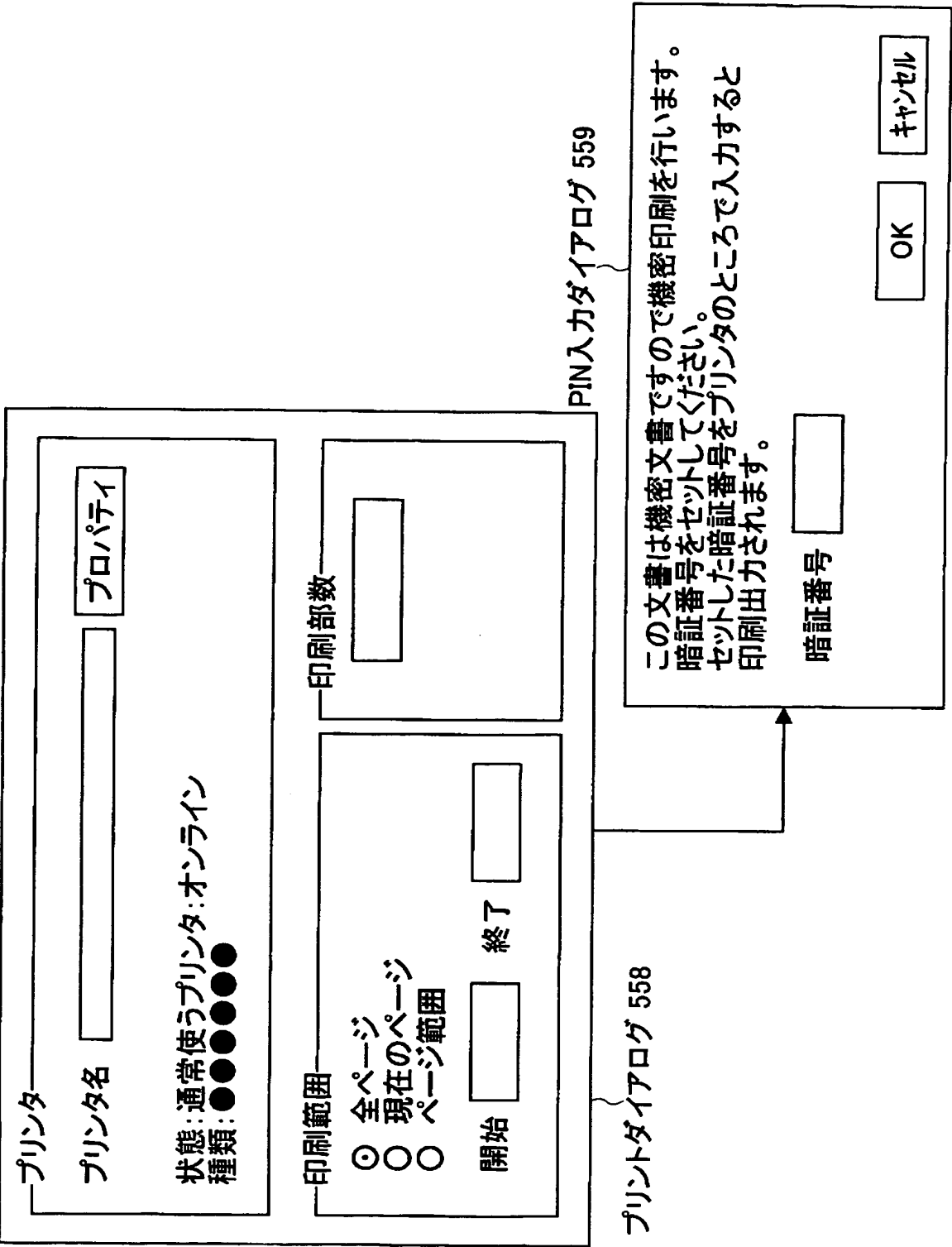
【図 20】

PACが設定されたドキュメントを印刷する際の処理を示す図



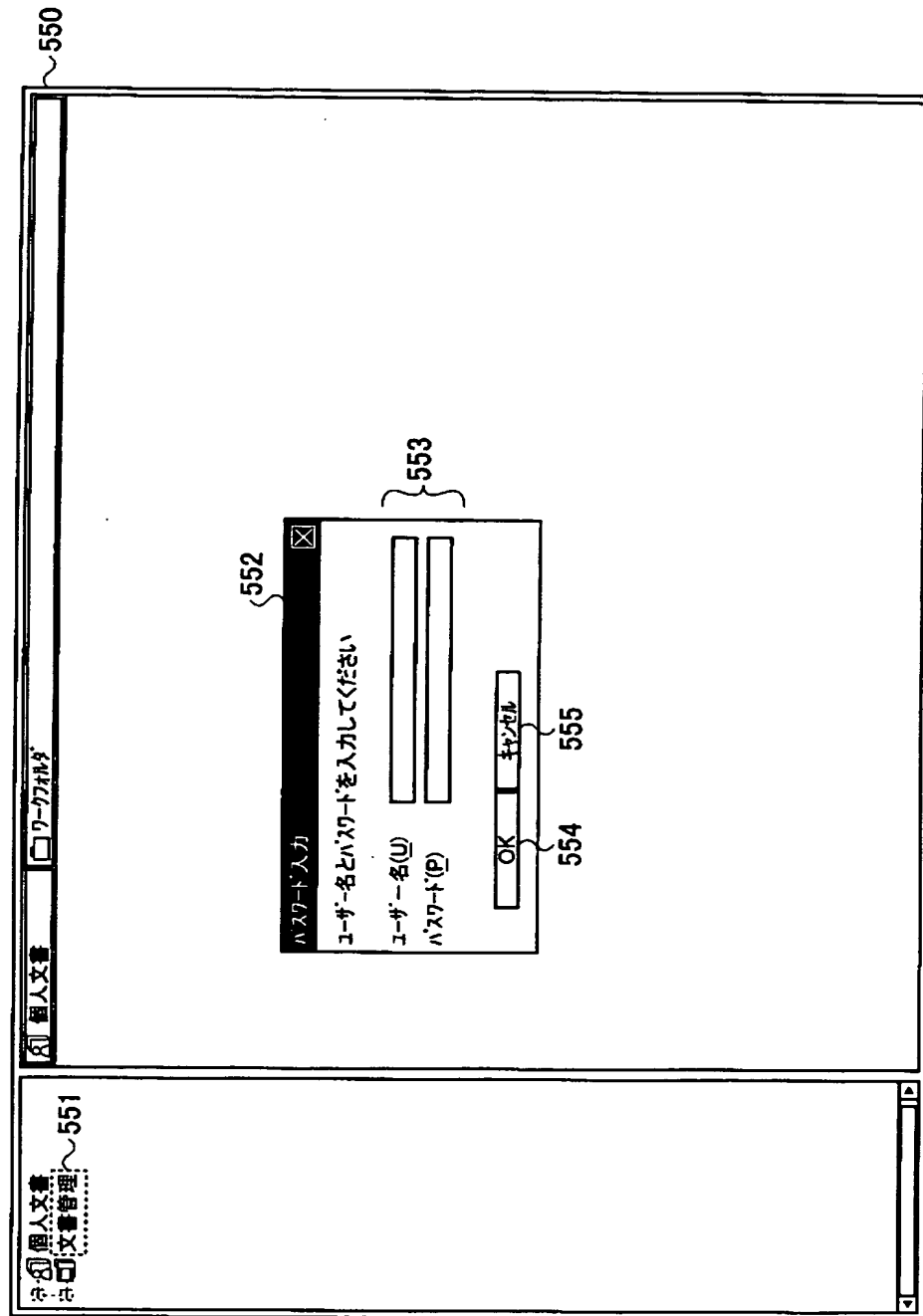
【図 21】

PIN入力のダイアログを示す図



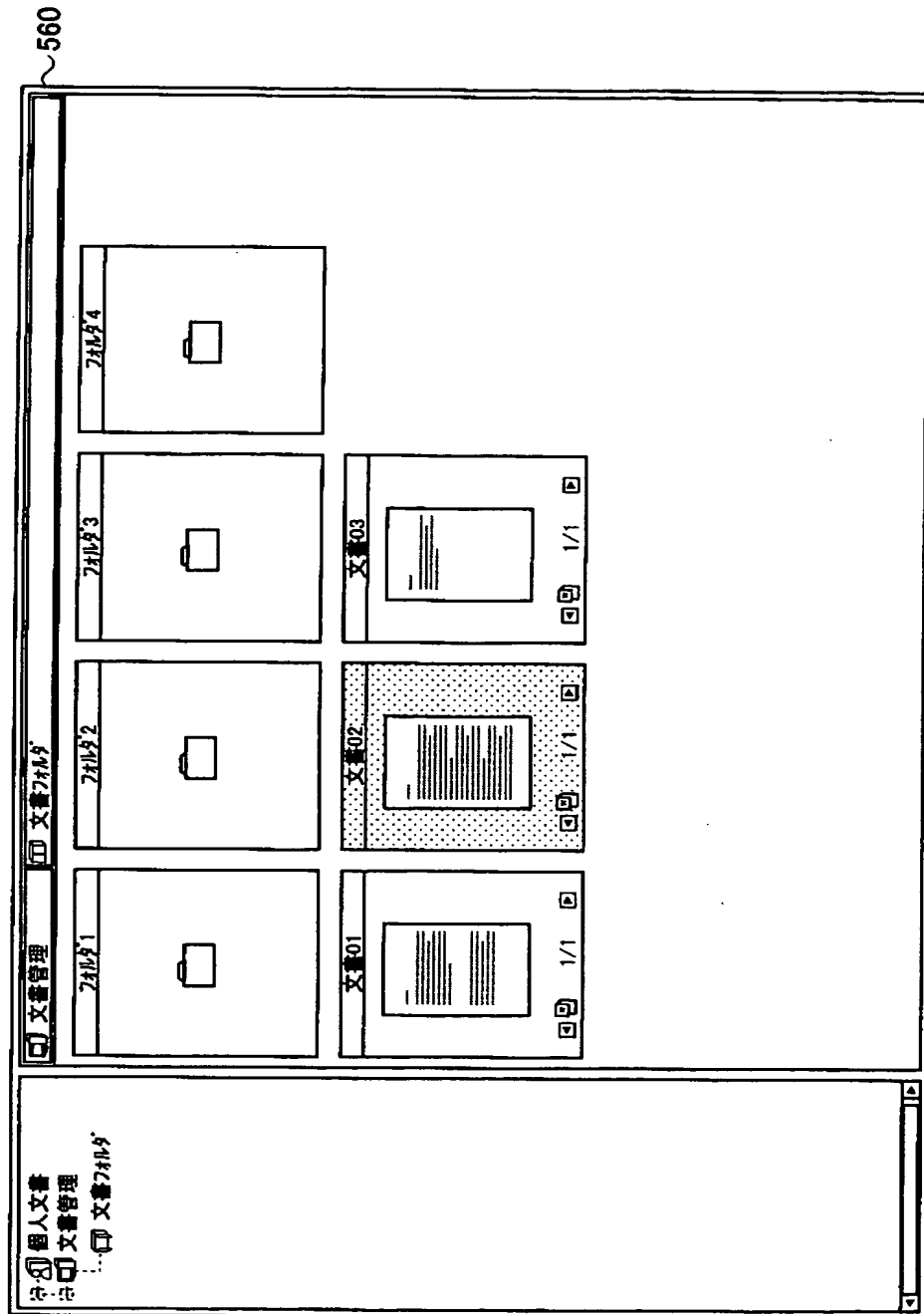
【図 22】

電子ファイル管理装置にアクセスした際に表示される画面例を示す図



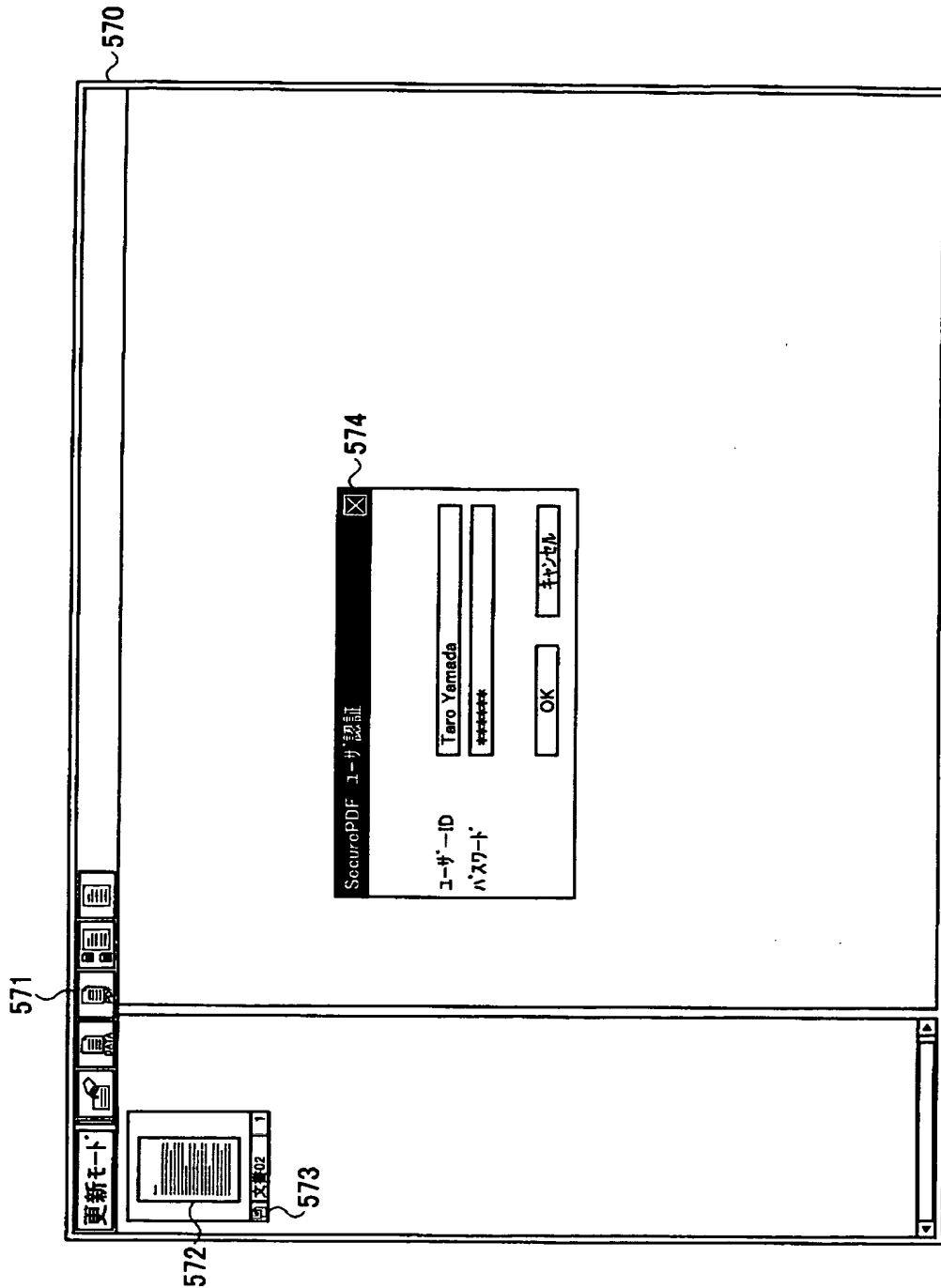
【図 23】

電子ファイル管理装置にて管理されるドキュメントの一覧を表示する
画面例を示す図



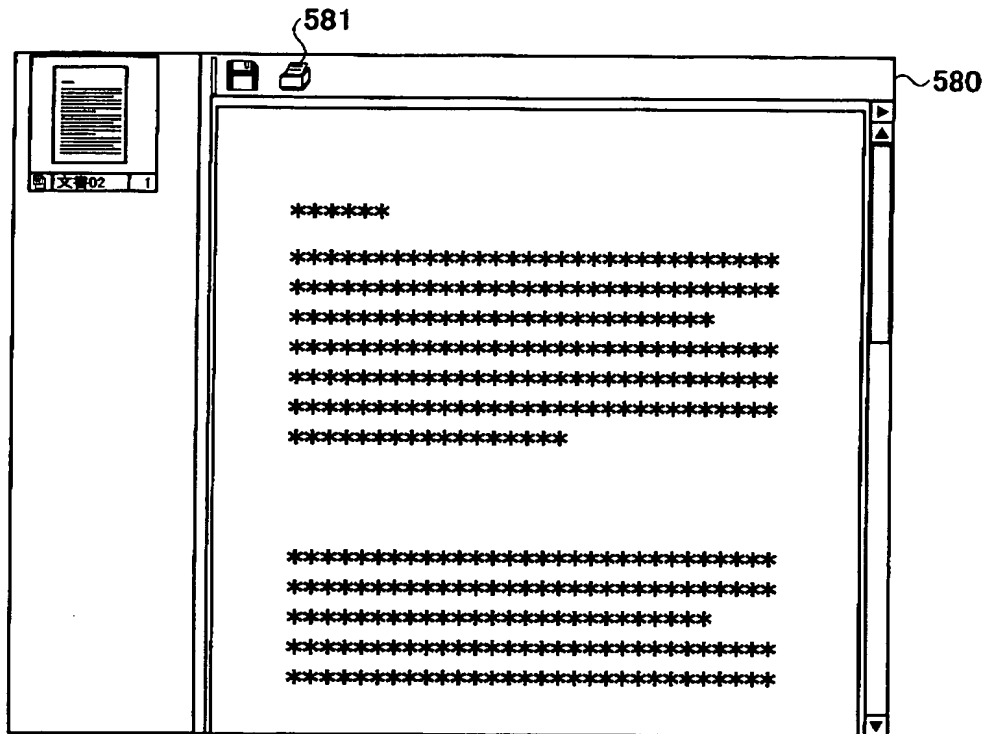
【図 24】

保護ドキュメントが提示されている画面例を示す図



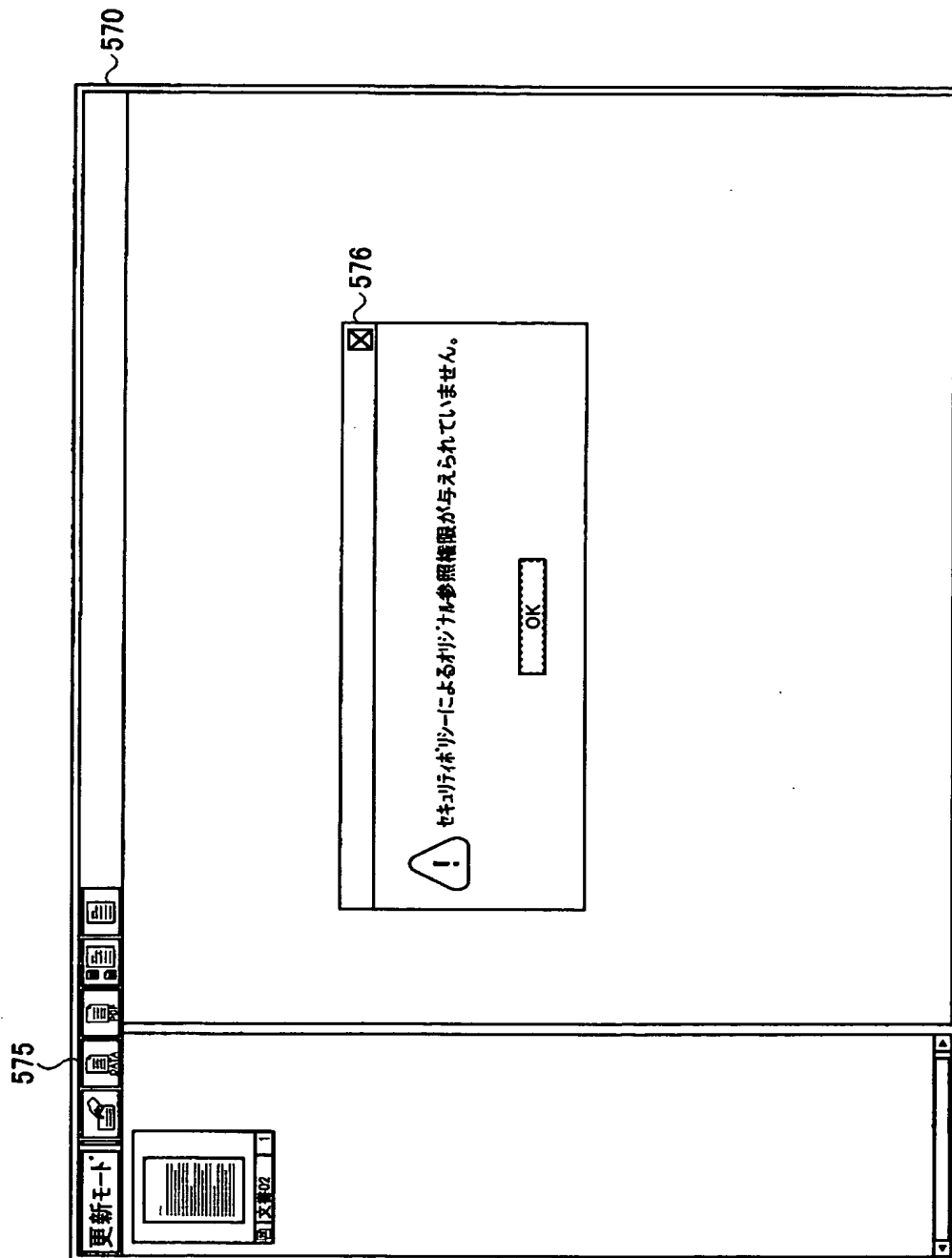
【図 25】

保護ドキュメントが開かれた状態を示す図



【図 26】

ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図



【書類名】 要約書**【要約】**

【課題】 本発明の課題は、セキュリティを必要とする技術文書などの電子ファイルを管理し、アクセス権限に応じて該電子ファイルに対するアクセス制御を行う電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法を提供することを目的とする。

【解決手段】 本発明の課題は、電子ファイルを格納する電子ファイル格納領域と、上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有する電子ファイル管理装置によって達成される。

【選択図】 図 1

特願 2003-318475

出願人履歴情報

識別番号

[000006747]

1. 変更年月日

2002年 5月17日

[変更理由]

住所変更

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー